DOI 10.37882/2223-2966.2023.05.35

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ СЕРВЕРНОЙ ЧАСТИ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ

Харазян Айк Арменович
ведущий разработчик, Высшая школа экономики, haykking@gmail.com

Аннотация. Современные реалии привели к тому, что все большую популярность приобретают распределенные приложения, доступ к которым пользователи получают посредством сетей передачи данных. Это обусловлено как развитием науки и техники, так и ростом популярности удаленной работы. При этом одной из важнейших задач функционирования данных приложения является обеспечение их безопасности, а в частности — безопасности серверной части приложения, где хранятся информационные базы, а также код серверной части программного обеспечения. Активное развитие технологий приводит к возникновению все новых методов обхода средств защиты, что требует реализации все более совершенны инструментов защиты для серверной части приложения. Это актуализирует выбранную тему исследования. Целью исследования является анализ современных методов защиты серверной части распределенных приложений. Задачи исследования: 1) рассмотреть существующие методы и средства обеспечения защиты серверной части распределенных приложений; 2) выполнить анализ рассмотренных методов и средств обеспечения защиты серверной части распределенных приложений; 3) привести рекомендации в плане использования, либо совершенствования проанализированных методов и средств обеспечения защиты серверной части распределённых приложений. При написании статьи использовался метод анализа научных источников и публикаций. Сделан вывод о том, что помимо организации защиты серверного окружения программного кода важно обеспечить защиты процедур в рамках его работы. Отмечено, что незначительные действия, например, обеспечение безопасного исполнения веб-запросов, устранение известных уязвимостей для ситуаций, когда используются стандартные фреймворки и т.д., могут принести огромные негативные последствия в плане работы серверной части распределенного приложения, что в совокупности принесет массу проблем его владельцам.

Ключевые слова: безопасность распределенного приложения, безопасность серверной части ПО, информационная безопасность, защита распределенного приложения.

MODERN METHODS OF PROTECTING THE SERVER PART OF DISTRIBUTED APPLICATIONS

H. Kharazyan

Summary: Modern realities have led to the fact that distributed applications are becoming increasingly popular, access to which users get through data networks. This is due to both the development of science and technology, and the growing popularity of remote work. At the same time, one of the most important tasks for the functioning of application data is to ensure their security, and in particular, the security of the server part of the application, where information bases are stored, as well as the code of the server part of the software. The active development of technologies leads to the emergence of new methods of bypassing protection tools, which requires the implementation of more and more advanced protection tools for the server part of the application. This actualizes the chosen research topic. The purpose of the study is to analyze modern methods of protecting the server part of distributed applications. Research objectives: 1) to consider the existing methods and means of ensuring the protection of the server part of distributed applications; 2) to analyze the considered methods and means of ensuring the protection of the server part of distributed applications; 3) provide recommendations in terms of using or improving the analyzed methods and means of ensuring the protection of the server part of distributed applications. When writing the article, the method of analyzing scientific sources and publications was used. It is concluded that in addition to organizing the protection of the server environment of the program code, it is important to ensure the protection of procedures within its work. It is noted that minor actions, for example, ensuring the secure execution of web requests, eliminating known vulnerabilities for situations where standard frameworks are used, etc., can bring huge negative consequences in terms of the operation of the server part of a distributed application, which together will bring a lot of problems to its owners.

Keywords: security of a distributed application, security of the server part of the software, information security, protection of a distributed application.

Современные реалии привели к тому, что все большую популярность приобретают распределенные приложения, доступ к которым пользователи получают посредством сетей передачи данных. Это обусловлено как развитием науки и техники, так и ростом популярности удаленной работы. При этом одной из важнейших задач функционирования данных приложения является обеспечение их безопасности, а в частности — безопасности серверной части приложения, где хранятся информационные базы, а также код серверной части программного обеспечения. Активное развитие технологий приводит к возникновению всё новых методов обхода средств защиты, что требует реализации все более совершенны инструментов защиты для серверной части приложения. Работа распределенных приложений подразумевает использование нескольких уязвимых точек, независимо от используемой архитектуры. Именно этот факт демонстрирует сложность обеспечения защиты — ведь в работе одного приложения участвуют одновременно клиентская часть, серверная часть и каналы передачи данных. Обеспечение защиты сервера является обязательным условием по причине размещения на нем основного состава программы — базы данных, а также исполняемого кода. Клиентская часть распре-

деленного приложения для злоумышленников представляет меньший интерес по причине того, что все она чаще всего выступает в роли инструмента отображения уже сформированного контента, и не выполняет никаких управленческих функций. Именно по той причине важным аспектом является обеспечение защиты именно серверной части распределенного приложения, что актуализирует выбранную тему исследования.

При рассмотрении методов обеспечения безопасности серверной части распределенных приложений в первую очередь следует определить состав наиболее актуальных уязвимостей, к которым относятся:

1. Инъекции в исполняемый код сервера, реализуемые в виде уязвимостей, которые злоумышленники используют при осуществлении процедур передачи непроверенных данных.
2. Уязвимости авторизации и аутентификации, возникающие в результате некорректной реализации данных механизмов на стороне сервера, за счет чего злоумышленники получают несанкционированных доступ.
3. Уязвимости вида «межсайтовый скриптинг», механизмы работы которых подразумевают внедрение вредоносного программного кода на стороне клиента, который при работе приложения будет осуществлять взаимодействие с серверной частью программного продукта.
4. Уязвимости контроля доступа, к числу которых необходимо отнести нарушение принципа предоставления наименьших привилегий пользователям, реализация обхода проверок контроля доступа, получение разрешений к чужим учетным записям, реализация повышения привилегий, а также получение доступа к метаданным.
5. Наличие небезопасных прямых ссылок на объекты, в результате чего возникает передача закрытых пользовательских данных в открытом виде.
6. Некорректное конфигурирование серверной части ПО в связи с отсутствие должного уровня безопасности, наличия ненужных служб, не отключения учетных записей по умолчанию, отсутствие должных обновлений ПО и т.д.
7. Уязвимости, позволяющие злоумышленникам осуществить отправку приложению HTTP-запроса, получив в результате необходимые сведения о работе приложения.
8. Использование элементов и API, содержащих уязвимости. Злоумышленники, выяснив, с использованием чего реализовано приложение в первую очередь проверяют наличие защиты от известных угроз и уязвимостей в программном коде [1].

Приведенный перечень нельзя назвать исчерпывающим. Для каждой конкретной ситуации, или конкретного подхода он может быть дополнен своими методами и подходами. Это в большей степени унифицированный список, который включает в себя базовый состав методов обеспечения информационной безопасности на стороне сервера. В частности, он может быть легко дополнен методиками защиты, применяемыми для конкретной серверной платформы — например, при устранении известных уязвимостей, либо применения наиболее подходящих для данной платформы инструментов обеспечения защиты.

На основании перечисленного перечня угроз серверной платформы распределенных приложений необходимо рассмотреть наиболее актуальные методы обеспечения должного уровня их безопасности.

Первым методом следует назвать использование аутентификации на основании SSH-ключей, которые реализуются в виде пары криптографических ключей. Один из данных ключей (публичный ключ) размещается в специальном каталоге сервера, а пользователь при прохождении процедуры аутентификации предоставляет второй (секретный) ключ. За счет реализации данного метода процедура аутентификации происходит полностью в зашифрованном виде. Для обеспечения полной защиты от использования уязвимостей аутентификации потребуется отключение данной процедуры на основании логина и пароля пользователя. Реализация данного метода осуществляется очень легко, как на стороне сервера, так и на стороне клиента [2].

Следующим методом следует упомянуть использование межсетевых экранов. Это довольно давно известный метод обеспечения защиты при работе в сети до сих пор не утрачивает своей актуальности. На стороне серверной платформы может быть использован как программный, так и аппаратный файрвол. В любом виде он будет осуществлять контроль состава сервисов, обладающих доступом к сети, и осуществлять либо блокирование, либо ограничение доступа для служб, сервисов и пользователей [3].

На сервере, где размещается серверная часть распределенного приложения, могут быть запущены несколько категорий различных сервисов. К ним относятся публичные сервисы, доступ к которым должны получать все категории пользователей, частные сервисы, доступ к которым должен быть предоставлен только избранным группам пользователей, и внутренние сервисы, доступ к которым должен быть предоставлен только внутренним сервисам сервера.

Использование межсетевого экрана позволяет обеспечить гарантии ограничений доступа к сервисам на основании описанных выше категорий, с возможностью гибкой настройки уровней и категорий доступа [4].

Для любой современной серверной платформы характерно наличие межсетевого экрана в составе базового набора программного обеспечения, так как это фактически дополнительный уровень безопасности, с возможностью гибкой настройки доступа. За счет ограничения числа доступных из вне сервисов достигается существенное снижения уровня вероятности взлома сервера. Использование межсетевого экрана является методов, довольно простым в инсталляции, однако требует корректного конфигурирования, так как можно заблокировать доступ к тем сервисам, к которым он в итоге должен быть предоставлен.

Следующим вариантом будет предложено использование виртуальных частных сетей — метода реализации безопасного соединения как между компьютерами, так и между компьютером и сервером. Реализация VPN позволяет в рамках открытых сетей реализовать защищенное соединение.

Эта методика реализуется довольно просто, главное выполнить конфигурирование VPN сервера, и установить специальный клиент. Однако использование его обусловлено в тех случаях, когда с приложением работает сотрудник организации, и ему необходимо предоставить доступ к защищаемой информации. В случае работы рядовых пользователей с программным продуктом, находящимся в открытом доступе, это будет реализовать не так просто, да и не каждый пользователь в данном случае захочет при каждом сеансе работы с приложением осуществлять дополнительное подключение [5].

Далее в качестве метода обеспечения защиты серверной части распределенных приложений следует будет представить инфраструктуру открытых ключей, а также шифрования SSL/TLS. Данная инфраструктура представляет собой систему, основное назначение которой заключается в создании, управлении и подтверждению сертификатов, которые используются в рамках процедур идентификации пользователей, а также шифрования сетевого взаимодействия. Применение сертификатов SSL и TLS может производиться с целью аутентификации пользователей, и последующей реализации защищенного сетевого взаимодействия.

Для реализации инфраструктуры открытых ключей необходимо конфигурирование специального удостоверяющего центра, который будет осуществлять процедуру управления сертификатами для серверов. Это позволит производить проверку подлинности не только на уровне пользователей, но и на уровне компонентов сетевой инфраструктуры, а также осуществлять шифрование передаваемых данных. За счет этого метода реализуется зашита от атак типа «атака посредника», при которых злоумышленниками выполняется имитация сервера внутри сети с целью перехвата передаваемых данных [6].

Каждый из серверов в рамках сетевой инфраструктуры можно настроить таким образом, что он будет доверять централизованному удостоверяющему центру. Получается, что любой сертификат, который будет подписан данным центром, будет считаться доверенным. В случае поддержки механизмов SSL/TLS шифрования приложениями и протоколами коммуникации будет предоставлена возможность защищенного взаимодействия между серверной и клиентской частью распределенного приложения без реализации VPN сети.

Данный метод может потребовать определенных усилий при его развертывании, а процесс управления сертификатами может в некоторой степени увеличить административную нагрузку. Однако он может стать более простым по сравнению с виртуальными сетями в том случае, когда речь идет о сетях передачи данных крупных предприятий и корпораций.

Представленные выше методы обеспечения безопасности направленны на обеспечение безопасности непосредственно сервера. Однако в рамках решения данного рода задач важно также производить анализ рассматриваемых систем, понимать механизмы потенциальных атак и изолировать критические компоненты инфраструктуры.

Одной из важнейших процедур в рамках обеспечения безопасности серверной части следует назвать аудит сервисов — проверки выполняемых на стороне сервера сервисов с целью выявления состава запущенных сервисов, определения задействованных в сетевой коммуникации портов и протоколов. Это позволит получить информацию для корректной настройки межсетевого экрана, а также отслеживать те сервисы, работа которых на текущий момент не требуется [7].

Получение объективной картины в вопросах перечня запущенных сервисов позволит проводить более качественную работу с точки зрения обеспечения защиты данных, так будет получен полный перечень запущенных приложений. На основании данного перечня, во-первых, можно будет изучить полный перечень типовых уязвимостей, а далее уже производить работы касаемо анализа конфигурирования файрвола, а также необходимо использования данного сервиса в работе серверной части.

Следующий метод подразумевает использование процедур аудита файлов, а также систем обнаружения вторжений. Процедура аудита файлов подразумевает подготовку «снимка состояния системы» после проведения базовых настроек и проведения последующих сравнений текущих настроек и файлов с данным снимком состояния. В случае обнаружения изменений производится анализ выполненных изменений с точки зрения их

влияния на обеспечение информационной безопасности. А применение систем обнаружения вторжений обеспечивает отслеживание неавторизованной активности в системе, что в определенной степени представляет собой автоматизированный вариант проведения аудита файлов и настроек [8].

С точки зрения информационной безопасности данные процедуры являются гарантом обеспечения уверенности отсутствия несанкционированных изменений в файловой системе сервера. За счет этого будут получены оперативные сведения в случае несанкционированной активности в системе, и принять меры по их устранению.

Что процедура настройки системы обнаружения вторжений, что проведение процедур аудита файлов представляют собой довольно непростое занятие, по той причине, что требует указать перечень нестандартных изменений на сервере. Также возможно потребуется указать те пути в файловой системе сервера, которые необходимо будет исключить при создании «снимка состояния» файловой системы, который будет применяться при последующих процедурах сравнения. Проведение процедур аудита файлов приводит к существенному увеличению нагрузки в вопросах администрирования сервера, однако позволяет обеспечить максимально высокую уверенность в том, что система не подвергалась каким-либо несанкционированным изменениям.

Еще одним из методов обеспечения защиты серверной части распределенного программного продукта необходимо назвать изолирование среды исполнения, при которой запуск каждого компонента осуществляется в собственной изолированной среде [9]. За счет этого достигается распределение отдельных компонентов программного продукта по различным серверам, либо настройку работы серверной платформы с использование отдельных изолированных контейнеров. За счет изоляции процессов повышаются возможности обеспечения защиты сервера за счет повышения устойчивости отдельных компонентов от атак извне.

Перечисленный состав методов представляет собой наиболее распространенные стратегии обеспечения информационной безопасности для серверной части распределенных программных продуктов. Однако следует выполнить рассмотрение представленных методик в разрезе двух аспектов — это рекомендации специалистов в области информационной безопасности в том плане, что реализация системы защиты должна происходить комплексно, а также с учетом того факта, что пользователями распределенных приложений являются самые различные категории людей, и чаще всего они не пожелают производить какие-либо дополнительные действия при работе с приложением со своего смартфона, планшета или ноутбука. Да и в случае с персональным компьютером мало кто захочет предварительно устанавливать VPN-подключение, или устанавливать дополнительные сертификаты.

Итак, с точки зрения обеспечения информационной безопасности на максимально высоком уровне требуется одновременное использование трех категорий защиты информации — технические, программные и организационные средства. Для большинства организаций организационные средства являются одним из основных инструментов защиты от каких-то несанкционированных действия пользователей, однако в случае с распределенными приложениями, да еще и общей категории пользования данные средства сложно будет применить, практически невозможно. К данной категории можно будет отнести только законы и нормативно-правовые акты, которые фактически будут действовать только в ситуациях, когда кто-то будет намеренно организовывать взлом сервера. Однако в данной ситуации злоумышленник уже будет иметь представление о том, что делает и какие последствия юридического характера будут его ожидать, поэтому данная категория средств защиты будет играть не столь важную роль при обеспечении защиты серверной части программного продукта. Именно по этой причине важно использовать две оставшиеся категории средств защиты.

В рамках аппаратных инструментов обеспечения защиты серверной части распределенных приложений в качестве наиболее эффективных следует отметить применение аппаратных межсетевых экранов, которые будут играть роль инструмента фильтрации входящего трафика с целью отсеивания потенциально опасного или нежелательного. Также сюда необходимо отнести инструменты обеспечения резервирования информации — дисковые массивы, аппаратные средства резервного копирования и т.д. Это в первую очередь защита от утери информации и возможность быстрого восстановления данных.

К программным инструментам необходимо отнести средства антивирусной защиты. Несмотря на использование средств межсетевого экранирования, применение средств антивирусного контроля все же необходимо. Также, как и необходимо применение инструментов поведенческого анализа, например, средств аудита и протоколирования событий информационной безопасности, в частности инструменты аудита событий и файлов. Однако реализация механизмов изолирования среды исполнения является также немаловажным инструментом обеспечения защиты.

На основании вышесказанного к инструментам защиты серверной части распределенных приложений необходимо в первую очередь относить инструменты

Рис. 1. Рекомендованный порядок реализации механизмов защиты серверной части распределённого приложения

аппаратного и программного характера. Процесс их реализации схематично представлен на рисунке 1.

Представленная схема демонстрирует оптимальный порядок конфигурирования инструментария по обеспечения защиты серверной части веб-приложения.

При конфигурировании инструментов защиты в рекомендованной последовательности будет получена возможность отслеживания работы необходимых приложений, задействованных в их работе протоколов, портов и файлов. Это все будет использовано при конфигурировании следующего элемента системы защиты и позволит пошагово пройти процедуру настройки всей системы защиты, не возвращаясь на каждом последующем этапе к предыдущим. За счет этого будет реализовано максимально корректная и качественная система обеспечения информационной безопасности серверной части распределенного приложения.

При этом помимо организации защиты серверного окружения программного кода важно обеспечить защиты процедур в рамках его работы. Например, обеспечение безопасного исполнения веб-запросов, устранение известных уязвимостей для ситуаций, когда используются стандартные фреймворки и т.д. Эти незначительные действия могут принести огромные негативные последствия в плане работы серверной части распределенного приложения, что в совокупности принесет массу проблем его владельцам.

В заключении необходимо отметить, что для каждого программного решения наиболее подходящий состав будет определяться опытным путем, а комплексное применение всех перечисленных методов будет не всегда быть подходящим решением, так как они в определенной степени будут оказывать влияние на скорость работы сервера, что является также немаловажным фактором. Таким образом, состав используемых средств и методов обеспечения защиты серверной части ПО определяется в первую очередь владельцем и администратором сервера.

ЛИТЕРАТУРА

1. Бабичев С.Л. Распределенные системы: учебное пособие для вузов / С.Л. Бабичев, К.А. Коньков. М.: Издательство Юрайт, 2023. 507 с.
2. Дубовик Е.В. Web на практике. CSS, HTML, JavaScript, MySQL, PHP для fullstack-разработчиков / Е.В. Дубовик, А.П. Никольский. М.: Наука и техника, 2021. 432 с.
3. Казарин О.В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О.В. Казарин, И.Б. Шубинский. М.: Издательство Юрайт, 2023. 342 с.
4. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. М.: Издательство Юрайт, 2023. 312 с.
5. Лаврищева Е.М. Программная инженерия и технологии программирования сложных систем: учебник для вузов / Е.М. Лаврищева. 2-е изд., испр. и доп. М.: Издательство Юрайт, 2022. 432 с.
6. Лащевски Т. Облачные архитектуры: разработка устойчивых и экономичных облачных приложений / Т. Лащевски, К. Арора, Э. Фарр, П. Зонуз. СПб.: ИД Питер, 2022. 320 с.
7. Лукьянов П.Б. Разработка и реализация портальных решений / П.Б. Лукьянов. М.: Прометей, 2020. 166 с.
8. Нестеров С.А. Основы информационной безопасности: учеб. пособие / С. А. Нестеров. Санкт-Петербург: Лань, 2017. 321 с.
9. Роберт М. Чистая архитектура. Искусство разработки программного обеспечения / М. Роберт. СПб.: ИД Питер, 2022. 352 с.
10. Чернышев С.А. Принципы, паттерны и методологии разработки программного обеспечения: учебное пособие для вузов / С.А. Чернышев. М.: Издательство Юрайт, 2022. 176 с.

Журнал «Современная наука: актуальные проблемы теории и практики»