УДК 004.056.5

МЕТОД РЕАЛИЗАЦИИ ПРИНЦИПА НУЛЕВОГО ДОВЕРИЯ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Слепынина М.М., Евдокимов И.В., студенты гр. ИБс-211, I курс

Научный руководитель: Киренберг А. Г., доцент (к.т.н.) ИИТМиА: Информационная безопасность

Кузбасский государственный технический университет имени Т.Ф. Горбачева

г. Кемерово

Аннотация

С развитием Интернета сетевая архитектура компании также претерпевает глубокие изменения, и границы между масштабами сетей (локальной и глобальной) становятся все более размытыми, что обусловлено появлением облачных сервисов. Все больше предприятий, компаний развертываются на облачном сервере, что увеличивает риск утечки данных между облачным сервером и внутренней сетью. В данной статье предлагается метод реализации принципа нулевого доверия для применения к приведенному выше сценарию, а именно – когда часть сервисов расположена в облачном хранилище. Метод нулевого доверия может обеспечить безопасный и надежный обмен данными при доступе внешнего сервера приложений к внутренней сети, эффективно защитить сетевые коммуникации и доступ к бизнесу, не затрагивая при этом первоначальные меры защиты внутренней сети, и сделать сеть компании более безопасной и контролируемой.

Ключевые слова: информационная безопасность, модель нулевого доверия, кибератака, внешняя сеть, внутренняя сеть, защита данных.

Введение

Традиционная структура сети обычно делится на внутреннюю и внешнюю сеть. На границе внутренней и внешней сетей устанавливается оборудование для защиты сетевой безопасности, такое как брандмауэр

(защитный экран между глобальным интернетом и локальной компьютерной сетью организации) и система обнаружения вторжений (IDS). Трафик данных между внутренней и внешней сетями проходит через эти устройства. Таким образом, традиционной архитектуре сетевой безопасности труднее гарантировать безопасность сети [1]. Существуют два основных риска безопасности:

- структура по умолчанию ориентирована на безопасность внутренней сети, в которой отсутствует эффективная защита от атак, в результате чего система безопасности такой сети может нарушаться за счет внутренних уязвимостей;
- безопасность внутренней сети во многом зависит от средств защиты со стороны внешней сети, а значит атака из внешней сети может перейти во внутреннюю сеть.

Некоторые серверы, такие как, например, веб-серверы (если они собственные, а не арендованные) располагаются во внутри брандмауэра или иначе – во внутренней сети. Брандмауэр отвечает за вопросы безопасности, а серверу нужно только обрабатывать бизнес-логику. Однако с быстрым развитием облачных вычислений многие компании начали переносить свой бизнес на облачную платформу Интернета, что изменило первоначальную сетевую архитектуру компании. Это привело к возникновению двух проблем безопасности.

Первая заключается в том, что облачные серверы передают данные через сети общего пользования, которой и является сеть Интернета, следовательно, риск атак возрастает.

Вторая – «размытие» границ сети [2]. Трудно провести четкую физическую границу между облачным сервером, внутренней сетью компании и Интернетом, что делает невозможным развертывание традиционных средств защиты сети. Традиционная концепция защиты сети, основанная на границах, также с трудом отвечает требованиям безопасности сложных сетевых структур.

Существующие решения

Для решения проблем, существующих в сценариях сетевой безопасности, появилась концепция безопасности с нулевым доверием (Zero trust). Модель нулевого доверия была впервые предложена аналитиком Forrester Джоном Киндервагом [3], а компания Google начала создавать проект BeyondCorp в 2011 году [4]. Каждый из проектов имеет свою направленность, но их основная концепция основана на "нулевом доверии", то есть все сети, трафик, пользователи и устройства по умолчанию не заслуживают доверия.

Поскольку, полагаясь только на такие механизмы защиты, как брандмауэры, IDS, антивирусы и т.д., невозможно обеспечить безопасность

границ сети, необходимо использовать более гибкие средства для установления новых логических границ для динамически изменяющейся сетевой инфраструктуры [5]. Благодаря идентификации и отслеживанию пользователей, терминалов, а также внедрению эффективных механизмов контроля доступа достигается многопараметрическая идентификация. Сетевая архитектура, созданная на этой основе, является архитектурой нулевого доверия [6]. В этой архитектуре идентификация стала новой границей сетевой безопасности, а ориентированная на идентификацию безопасность с нулевым доверием станет общей тенденцией развития сетевой безопасности как таковой.

В архитектуре с нулевым доверием всем пользователи и устройствам по умолчанию не доверяют. Прежде чем устройства и пользователи смогут получить доступ к данным, они должны пройти аутентификацию и авторизацию [7]. Как передовая концепция сетевой безопасности, нулевое доверие имеет различные методы реализации в конкретных сценариях применения.

Существующее стандартное решение по обеспечению безопасности идентификации на основе нулевого доверия [10] предоставляет людям, устройствам и приложениям цифровые идентификаторы и создает механизм контроля доступа, ориентированный на идентификацию. Это решение включает в себя динамическую доверенную платформу управления доступом, интеллектуальную доверенную платформу идентификации и токены для смартфонов. Принцип "Zero Trust Security Architecture" может эффективно решить проблему безопасности доступа к информации в новых бизнес-сценариях, таких как облачные вычисления. Однако его применение требует большого количества оборудования и сложной сетевой структуры и в основном ориентировано на требования приложений для центров обработки и платформ больших объемов данных, и не подходит для требований сетевой безопасности малых и средних компаний.

Метод реализации нулевого доверия, предложенный в данной статье, в основном ориентирован на сценарий применения, когда пользователи получают доступ к данным интрасети через сервер приложений, развернутый на облачном сервере, а приложения в свою очередь, должны взаимодействовать с интрасетью компании. Такое решение подходит для малых и средних компаний.

Предлагаемое решение

Структура схемы

Часть бизнес-логики (син. «логика предметной области») – это реализация правил и ограничений автоматизируемых операций) требует от внешнего облачного сервера доступа к данным интрасети (частная корпоративная сеть, использующая программные продукты и технологии Internet, например, Web-сервер) компании. Чтобы решить проблему безопасности в "Zero Trust Security Architecture", перед использованием бизнес-логики требуется аутентификация безопасности, и только безопасные запросы доступа имеют право вызывать данные из интрасети. Этот метод основан на принципе, который предполагает нулевое доверие для всех устройств, получающих доступ к данным интрасети, что поможет эффективно защитить сетевые коммуникации и внешний доступ, не полагаясь на механизм физической безопасности сети. Схема принципа нулевого доверия представлена на рисунке 1.

Общая система состоит из Token Generate Center (TGC), сервера приложений, сервера оценки и шлюза.

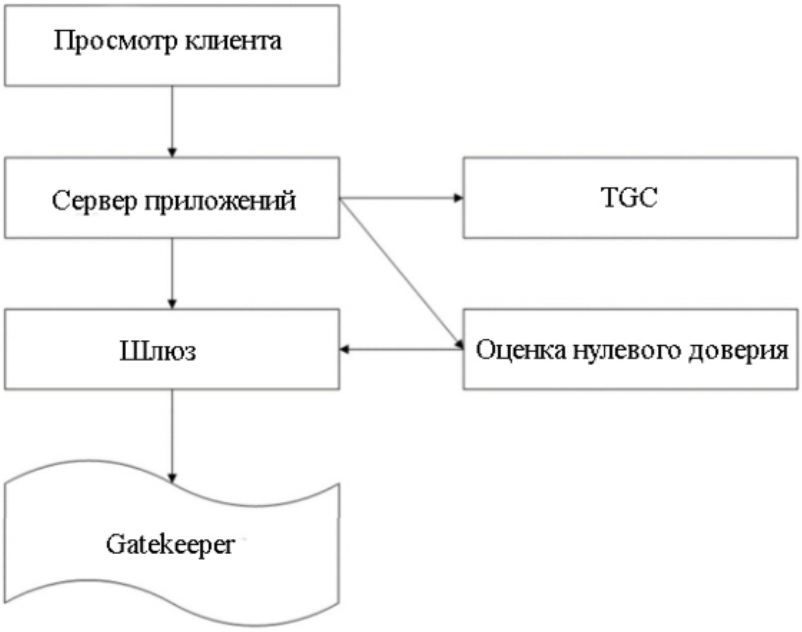

Рисунок 1. Блок-схема архитектуры нулевого доверия

В представленной схеме сервер приложений – это сервер, на котором установлено программное обеспечение, сертификаты инициализации, клиентское программное обеспечение с нулевым доверием и т.д. Клиент сообщает информацию о безопасности сервера, такую как уязвимости информационной системы.

Сервер оценки нулевого доверия в основном используется для оценки состояния сервера приложений. Он получает информацию о безопасности от сервера приложений, оценивает информацию и отправляет результаты на

шлюз. Сервер приложений подключается и взаимодействует с сервером оценки нулевого доверия через SSL

TGC – это сервер управления токенами, используемый для генерации информации о них для приложений. Он принимает SSL-соединение сервера приложений, генерирует токены для запросов и управляет ими.

Шлюз, который расположен между сервером приложений и привратником, используется для решения вопроса о возможности доступа сервера приложений к привратнику. Когда клиент получает доступ к данным интрасети через сервер приложений, сервер оценки нулевого доверия выполняет оценку безопасности сервера приложений и отправляет рассчитанный балл на шлюз, чтобы определить, разрешить ли серверу приложений доступ к интрасети. Шлюз принимает результат оценки сервера приложений от сервера оценки нулевого доверия. Серверы с результатом оценки более 60 разрешены для прохождения, а серверам с результатом менее 60 запрещено запрашивать.

Gatekeeper – это беспроводное бесконтактное устройство контроля доступа и аутентификации, которое позволяет пользователю автоматически заблокировать свой компьютер на расстоянии.

Процесс оценки нулевого доверия

Элементы оценки включают в себя: требуемые программы (в т.ч. программы обнаружения слабых паролей, обнаружения подозрительных веб-сайтов, обнаружения конфигураций, обнаружения уязвимостей хоста, обязательного контроля доступа и т.д.); уязвимости безопасности операционной системы; уязвимости безопасности сети; порты высокого риска; Процесс оценки показан на рисунке 2.

Если принцип работы большинства приведенных способов контроля предельно понятен, то в случае с Brute force protection (метод угадывания пароля или ключа, используемого для шифрования, предполагающий систематический перебор всех возможных комбинаций символов до тех пор, пока не будет найдена правильная комбинация) стоит заострить своё внимание на том, что производится защита от атак с одного IP-адреса на одну учетную запись пользователя.

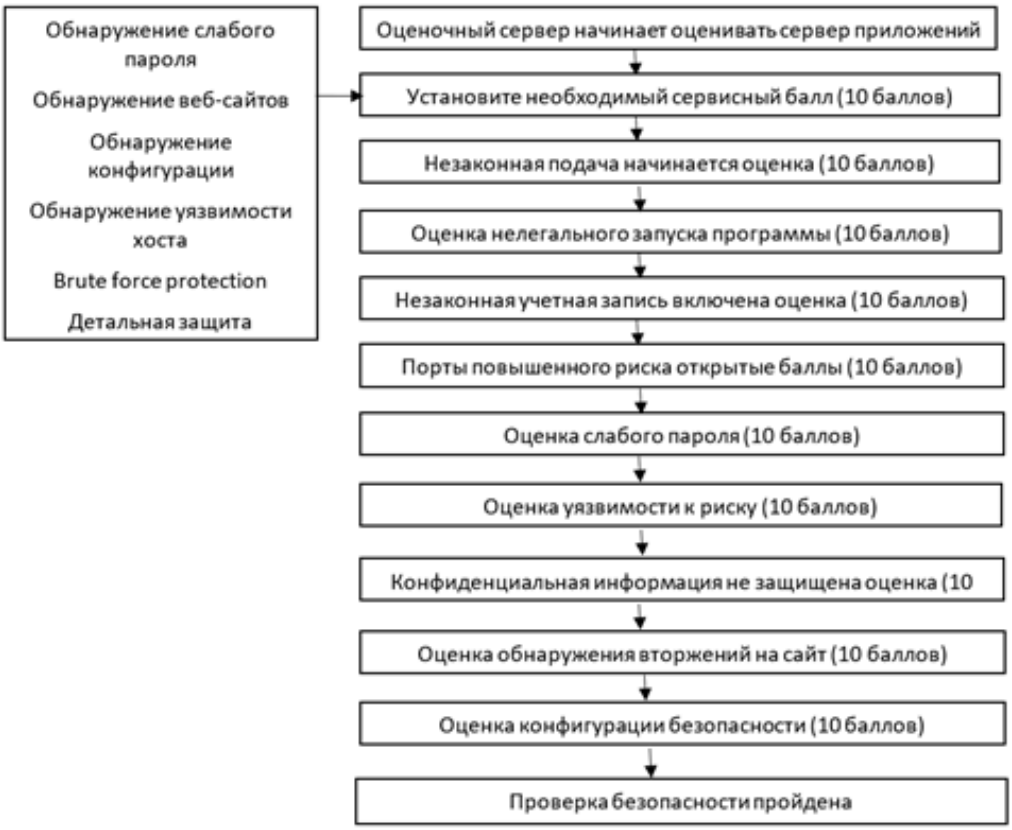

Рисунок 2. Процесс оценки нулевого доверия.

Рабочий процесс

Общий рабочий процесс обмена данными между внутренними и внешними сетями на основе архитектуры нулевого доверия показан на рисунке 3. Работа всего процесса также требует поддержки системы сертификатов. Сервер оценки, TGC, шлюз и сервер приложений используют один и тот же корневой сертификат, включая SSL-коммуникацию и цифровую подпись токена. Сертификат сервера приложений должен быть установлен и настроен первым, а шлюз должен проверить цифровую подпись при проверке токена. Рабочий процесс каждой части выглядит следующим образом:

- сервер приложений устанавливает: деловое основное программное обеспечение, программное обеспечение безопасности (включая, но не ограничиваясь всем программным обеспечением, упомянутым в оценке) и программное обеспечение клиента прокси с нулевым доверием;

- программное обеспечение прокси-клиента регулярно отправляет информацию о безопасности сервера приложений на сервер оценки нулевого доверия, включая различную информацию о безопасности, необходимую в

процессе оценки, а также информацию о результатах сканирования программного обеспечения;

- сервер оценки безопасности получает информацию о безопасности сервера приложений и другую информацию машины. Оценивает, выставляет баллы, и отправляет оценку на шлюз. Шлюз оценивает результат и решает, разрешить ли серверу приложений пройти проверку;

- шлюз получает результаты оценки сервера приложений по критериям безопасности, устанавливает состояния для каждого сервера приложений, сохраняет его соответствующие параметры (IP, Mac, оценка, время оценки, период действия), перезаписывает предыдущие результаты оценки после поступления последующих результатов. Шлюз обрабатывает каждый результат оценки в {IP, pass} или {IP, reject} и сохраняет его в ядре управления сетью, чтобы он мог быть выпущен или перехвачен, когда ядро обрабатывает запрос сервера приложений;

- сервер приложений использует предустановленный сертификат для установления SSL-связи с TGC и сервером оценки нулевого доверия для выполнения соответствующих задач связи. Серверу приложений необходимо получить маркер от TGC, а затем использовать этот маркер для запроса данных из интрасети;

- сервер TGC используется для генерации, распределения и управления токенами, а также для управления и использования их вместе со шлюзом;

- после того, как сервер приложений получает маркер, он подписывает его в URL для запроса внутренних данных от шлюза или привратника;

- после того, как шлюз получает запрос от сервера приложений, он просматривает локальную таблицу пропусков в соответствии с IP. Если результатом является "{IP, pass}" и его маркер имеет разрешение на доступ к данным, то вход в интрасеть разрешен. В противном случае запрос будет отклонен;

- после того, как сервер приложений запрашивает вход в gatekeeper, он получает ответ из внутренней сети, а шлюз возвращает ответ серверу приложений, и доступ на этом завершается.

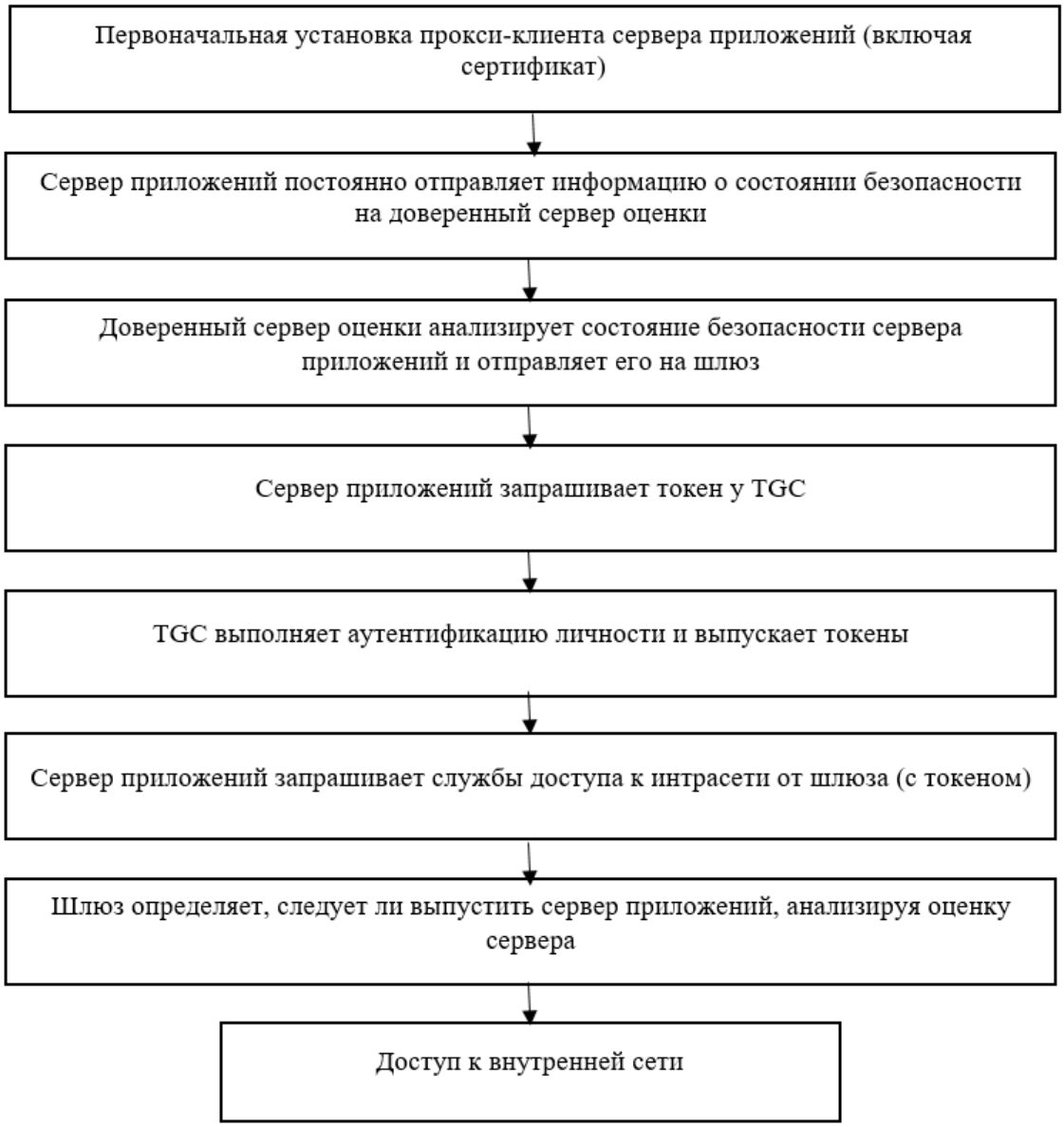

Рисунок 3. Рабочий процесс принципа нулевого доверия

Заключение

Таким образом, предложенный в данной статье метод, в отличии от традиционного, гарантирует безопасность обмена данными между сервером приложений внешней сети и внутренней сетью путем построения набора механизмов контроля доступа на основе архитектуры нулевого доверия в существующей сети компании, а также реализует гибкость процесса доступа путем динамической оценки состояния сервера. Она может легко предотвратить небезопасный доступ к внутренней сети компании, эффективно защитить её данные и доступ к бизнесу и сделать сеть более безопасной и контролируемой.

Список литературы:

1. Liu, Q. Data center security protection in the industry based on zero-trust architecture. Security & Informatization. 2018; 12:107-109.
2. Yang, Z., Jin, M., Zhang, X. Research on Security Technology of Zero Trust in Cloud Business. Information Security and Communications Privacy. 2020; 3: 91-98.
3. Kindervag, J. Build security into your network's DNA: the zero-trust network architecture. Forrester Research Inc. 2010; 1-26.
4. Ward, R., Beyer, B. Beyondcorp: A new approach to enterprise security. Login the Magazine of USENIX &Sage. 2014;39(6):6-1.
5. Liu, Z. Discussion on the construction of network information security system for digital transformation enterprises under the new normal. Cyberspace Security. 2018;9(11): 80-87.
6. Zuo, Y. Zero-trust architecture: a new paradigm for network security. Financial Computerizing. 2018; 11: 50-51.
7. Zeng, H.; Discussion on Network Security Model and Zero-trust Practice. Computer Products and Circulation. 2020;7: 48.
8. Zhong, X., Guo, W., Ma, Y., Wang, M. Airport Network Security Protection Scheme Based on Zero Trust Security Architecture. Journal of Civil Aviation, 3(03): 2019;114-116+107.
9. Lin, C., Li, X. Application and research of zero-trust architecture in the construction of network security in colleges and universities. Computer Products and Circulation. 2019; 9:209-210.
10. Cai, R., Zhang, X. Zero Trust Based Identity Security Solution. Information Technology & Standardization. 2019; 9:46-49.
11. Xue, Z., Xiang, M. Data Center Security Protection under Zero-Trust Security Model. Communications Technology. 2017; 50(06): 1290-1294.