защищенности, функциональности, производительности и удобства использования. Выбор нужных настроек безопасности осуществляется на основании методов поддержки принятия решений с использованием многомерной информации, хранящейся в ОЦИБ (Рис. 1). Адаптивный ОЦИБ оценивает состояние защищенности банковской организации и динамически формирует некоторую консолидированную оценку защищенности АБС. По результатам этой оценки ОЦИБ вырабатывает управляющее воздействие — какие настройки безопасности должны быть применены в настоящий момент:

— минимальные настройки безопасности — слабая защита, высокое удобство пользования;

— усиленные настройки безопасности — сильная защита, низкое удобство пользования;

— стандартные настройки безопасности — компромиссный вариант между первыми двумя.

Выбор настроек в зависимости от внешних факторов позволит влиять на поведение системы и тем самым повысить одновременно защищенность и удобство пользования АБС, что подтверждено результатами моделирования и рабочим экспериментом.

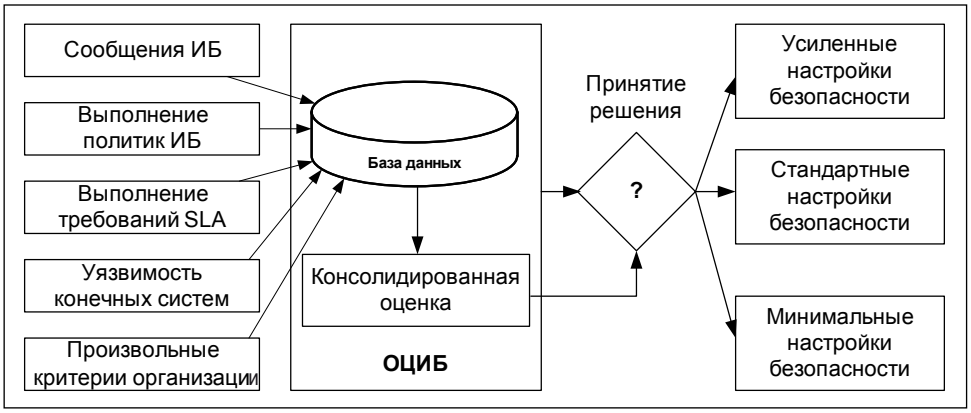

Рис. 1. Схема работы адаптивного ОЦИБ

Д. О. Ковалев, Н. Г. Милославская

МЕЖКОРПОРАТИВНАЯ КОРРЕЛЯЦИЯ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автоматизированные банковские системы (АБС) исторически считались закрытыми средами. Однако сегодня доступ к определенной банковской информации предоставляется широкому кругу лиц при помощи служб дистанционного банковского обслуживания (ДБО). ДБО реализуется посредством банковских интернет-приложений. Данные приложения позволяют клиентам банка управлять своим банковским счетом и пользоваться другими финансовыми услугами, не отходя от персонального компьютера. Общение с подобными приложениями происходит в интерактивном режиме через веб-сайт, размещенный в сети Интернет. Поскольку к веб-сайту могут обращаться как законные пользователи, так и злоумышленники, необходимо использование соответствующих средств защиты. При этом базовые механизмы защиты — аутентификация пользователей, шифрование данных и межсетевое экранирование — часто оказываются неэффективными перед такими атаками, как манипуляция параметрами, межсайтовый скриптинг и инъекция SQL-кода.

В процессе подобных атак злоумышленник использует уязвимости интернет-приложений, в результате получая над ними контроль. Необходимую защиту в этом случае способен предоставить комплексный подход к обеспечению ИБ с использованием ОЦИБ.

ОЦИБ может оценить всю совокупность сообщений, связанных с тем или иным событием ИБ, и принять правильное управляющее решение, например отправить на межсетевой экран команды, которые заблокируют атаку злоумышленника. При этом в работе ОЦИБ могут случиться ложные срабатывания и пропуски действительных атак (ошибки первого и второго рода). Любая неверная идентификация инцидента приведет к нежелательным для банка последствиям: в одном случае банк будет признан как неблагонадежный (если учетная запись пользователя будет скомпрометирована) либо как ненадежный (если пользователь из-за ложного срабатывания не получит доступ к своей учетной записи). Поэтому в случае использования интернет-приложений необходимо значительно повысить точность выявления сетевых атак.

В качестве способа повышения точности выявления атак предлагается использование базы данных репутаций (БДР) в рамках ОЦИБ и реализация межкорпоративной корреляции событий ИБ между различными организациями. Под репутацией в данном контексте понимается общественное мнение об IP-адресах в Интернете. Если заданный IP-адрес ранее был замечен при проведении атаки в Интернете, то он, скорее всего, либо принадлежит злоумышленнику, либо заражен вредоносным ПО и, как следствие, репутация у него плохая. Если же IP-адрес в противоправных действиях замечен не был, то это не влияет на его репутацию.

Для успешной реализации такого подхода ОЦИБ должен, с одной стороны, собирать информацию о репутации (ИоР), с другой стороны, передавать ее другим участникам обмена ИоР. Это может быть реализовано двумя способами. Первый способ подходит для закрытого ограниченного числа организаций, участвующих в информационном обмене. В этом случае каждый ОЦИБ напрямую обменивается ИоР со всеми остальными ОЦИБ, участвующими в обмене. Данный способ подходит для ОЦИБ дочерних организаций или ОЦИБ организаций, принадлежащих одному холдингу. Второй способ подразумевает отрытое участие в обмене, при котором в Интернете размещается единая база данных, содержащая ИоР. Каждый ОЦИБ, участвующий в информационном обмене, взаимодействует напрямую с БДР. ОЦИБ отправляет ИоР IP-адресов в Интернет, которую он собрал в ходе своей работы, а также получает информацию, хранящуюся в Интернете в БДР.

При этом очевидно, что в любом из приведенных вариантов обмен информацией должен производиться по защищенному протоколу (SSH/HTTPS) и должны использоваться соответствующие средства аутентификации ОЦИБ и контроля доступа ОЦИБ к БДР. Также важно, чтобы эта база динамически обновлялась и не содержала идентификаторов отправителя, поскольку это может косвенно нанести ущерб реноме организации. Рекомендуемый для хранения в БДР набор данных, который обеспечит анонимность участникам обмена, включает в себя IP-адрес или доменное имя нарушителя в Интернете, идентификатор протокола сетевого/транспортного уровня модели взаимодействия открытых систем (ВОС) и/или номера портов источника и назначения на транспортном уровне модели ВОС и ответную реакцию на событие ИБ.

Участие в обмене ИоР может быть односторонним. В этом случае ОЦИБ будет только получать информацию из БДР и не отправлять данные, зафиксированные локально. Однако наибольший эффект от использования БДР будет достигнут при наибольшем количестве ОЦИБ, активно обновляющих сведения об атакующих в Интернете.

После того как ОЦИБ получает ИоР, происходит межкорпоративная корреляция событий ИБ. Непосредственно сама ИоР никак не помогает в выявлении атак на информационные системы, поскольку это является задачей СЗИ, находящихся под управлением ОЦИБ. В случае

выявления угрозы ИБ локально ОЦИБ анализирует идентификатор нарушителя, связанный с обнаруженной угрозой на предмет соответствия БДР (рис. 1). В случае если прослеживается взаимосвязь, например IP-адрес источника пакетов был уже неоднократно замечен при проведении атак в Интернете, рейтинг значимости выявленного события ИБ значительно повышается.

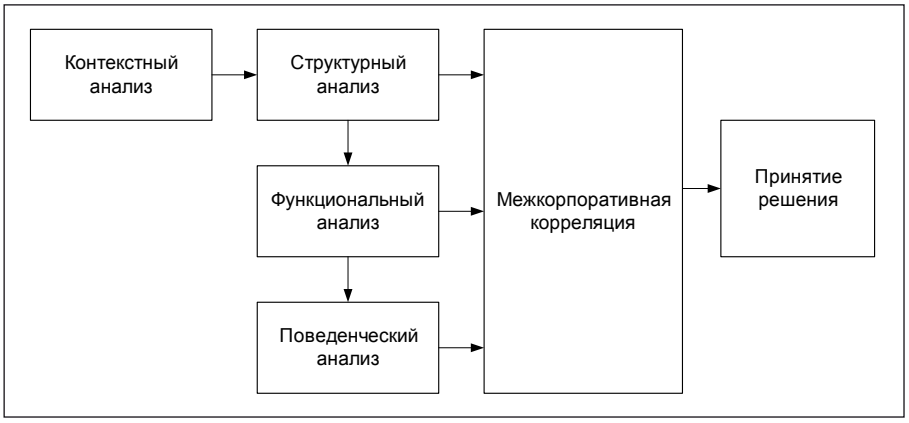

Рис. 1. Схема работы межкорпоративной корреляции

Рейтинг значимости события ИБ в рамках ОЦИБ отражает важность связанной с этим событием угрозы ИБ. Чем более важное событие ИБ, тем меньше вероятность того, что имеет место ложное срабатывание. Таким образом, на основании результатов межкорпоративной корреляции в значительной степени снижается количество ложных срабатываний и, как следствие, повышается эффективность работы ОЦИБ.

И. Ю. Коркин, Т. В. Петрова, А. Ю. Тихонов

МЕТОД ОБНАРУЖЕНИЯ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Новые процессоры Intel и AMD поддерживают режим аппаратной виртуализации (AB) [1, 2], расширяющий возможности как для легитимного, так и для вредоносного программного обеспечения (ВПО).

Необходимо отметить, что штатные средства обнаружения запущенного монитора виртуальных машин (МВМ) в компьютерных системах отсутствуют, а опубликованные — непереносимы [3], уязвимы к обнаружению и, как следствие, неэффективны.

В связи с этим авторами решалась задача разработки средств, позволяющих с достаточной степенью надежности решать вопрос о присутствии или отсутствии МВМ в компьютерных системах даже в случае активного противодействия их обнаружению.

Поскольку упомянутые процессоры обрабатывают возникающие в ОС события с помощью монитора виртуальных машин, с целью обнаружения факта их работы в современных компьютерах был разработан специальный метод, основанный на динамическом изменении числа выполняемых инструкций.