С. А. Петров, П. Б. Хорев

ПОСТРОЕНИЕ СИСТЕМЫ АДАПТИВНОЙ ЗАЩИТЫ НА БАЗЕ МНОГОАГЕНТНОЙ СИСТЕМЫ

В широком смысле информационная система (ИС) — это совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать надлежащих людей надлежащей информацией [1]. В узком смысле ИС называют только подмножество компонентов, включающее базы данных, СУБД и специализированные прикладные программы. ИС в узком смысле рассматривают как программно-аппаратную систему, предназначенную для автоматизации целенаправленной деятельности конечных пользователей, обеспечивающую, в соответствии с заложенной в нее логикой обработки, возможность получения, модификации и хранения информации [1]. В любом случае, основной задачей ИС является удовлетворение конкретных информационных потребностей в рамках конкретной предметной области. Здесь и далее будем рассматривать ИС в узком смысле — как программную систему.

Можно выделить компоненты, которые входят практически в любую ИС: СУБД, веб-сервер, специализированные прикладные программы. Каждый из компонентов является абстрактным хранилищем информации. Рассматривая конкретную ИС, каждый из компонентов можно описать более подробно и выделить как технологическую платформу, так и более специфичные настройки. Например, можно указать: СУБД — Microsoft SQL Server 2012, веб-сервер — Microsoft IIS, специализированные прикладные программы — платформа Microsoft Dynamics CRM 2011.

Для работы ИС должны быть сконфигурированы все ее компоненты, настроены механизмы авторизации и аутентификации, в БД может содержаться справочная информация, могут быть заданы начальные параметры запуска служб и т. д. Данные начальные настройки программной системы можно считать эталонными. Все эти настройки хранятся в системе и могут изменяться в процессе функционирования ИС.

Каждый из компонентов отвечает за определенный набор действий, например, СУБД — за доступ к БД, за механизмы синхронизации и др., веб-сервер — за обработку веб-запросов, специализированные прикладные программы созданы для решения более специфичных задач пользователя — учета заказчиков и обработки их запросов и т. д. В процессе функционирования ПС каждый из ее компонентов выполняет определенные действия, которые можно протоколировать для последующего анализа. Анализ файлов аудита используется для выявления событий несанкционированного доступа (НСД) и возможных причин. Стоит заметить, что злоумышленник может получить доступ к файлам аудита и удалить записи, которые связаны с его присутствием в системе.

Резюмируя описанный выше состав ПС и ее функционирование, можно сделать следующие допущения:

- любая ИС состоит из компонентов;
- все компоненты имеют начальные настройки;
- каждый из компонентов отвечает за определенный набор действий;
- в процессе функционирования ИС настройки могут изменяться;
- в процессе функционирования ИС компоненты выполняют действия;
- изменения настроек и выполнение действий можно протоколировать.

Как было отмечено выше, функционирование системы с точки зрения программного обеспечения — это работа компонентов с учетом своих настроек. Можно выделить следующие причины НСД [2]:

- ошибки конфигурации (прав доступа, межсетевых экранов, ограничений на массовость запросов к базам данных);

- слабая защищенность средств авторизации (хищение паролей, смарт-карт, физический доступ к слабо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников);
- ошибки в программном обеспечении;
- злоупотребление служебными полномочиями (воровство носителей с резервными копиями, копирование информации на внешние носители при праве доступа к информации);
- прослушивание каналов связи при использовании незащищенных соединений внутри ЛВС;
- использование клавиатурных шпионов, вирусов и троянов на компьютерах сотрудников для деперсонификации.

Независимо от причины несанкционированного доступа, сам доступ (с технической точки зрения) — это выполнение действий компонента или его переконфигурирование. Любое неправомерное действие (техническое) использует настройки и/или действия компонентов. Например, для удаленного подключения к серверу можно «подсмотреть» пароль, но само подключение требует выполнения действия — вызова компонента проверки прав. Если же злоумышленник проник на Windows-сервер, добавил учетную запись «intruder» в MS SQL, с ее помощью подключился к БД и считывает базу логинов и паролей системы, то в момент чтения он использует настройку: «intruder» имеет доступ к БД, и использует действие «считать записи из таблицы».

В подавляющем большинстве атак изменение настроек и/или вызов действий происходит в достаточно короткий промежуток времени и достаточно часто. Это связано с тем, что при проникновении в систему злоумышленник хочет как можно быстрее осуществить свою цель, почистить файл аудита и «скрыться». Само проникновение также создает дополнительную, «нестандартную», нагрузку на систему. Определение этой нагрузки и есть задача систем адаптивной защиты. Определение начала вторжения — основная задача для систем защиты, так как атаку лучше предотвратить, чем потом устранять ее последствия. Вероятно, из-за высокой скорости осуществления атаки администратор не успевает отреагировать и что-либо противопоставить ей на раннем этапе. Для построения системы защиты можно использовать подходы искусственного интеллекта, а именно многоагентные системы.

Основными особенностями многоагентных систем, которые позволяют эффективно их использовать в системах сетевой безопасности, являются [2]:

1. Гибкость и масштабируемость, за счет создания новых агентов и их размещения на новых узлах сети. Поэтому такие системы легко адаптируются к любой сетевой архитектуре и адекватно отвечают на изменения в конфигурации сетевого оборудования.

2. Экономичность, так как многоагентная система равномерно распределена по всему периметру защиты. Эта особенность обеспечивает оптимальное распределение вычислительных ресурсов сети.

3. Повышенная отказоустойчивость. Так как агенты могут существовать самостоятельно и они распределены на всех узлах сети, то есть система защиты не имеет центра, то атаковать ее будет сложнее, нежели сеть с централизованным сервером защиты. Распределенная по сети информация и распределенная защита требуют от злоумышленника проведения одновременной атаки многих узлов.

4. Возможность централизованного администрирования. Со всеми агентами можно «контактировать» по заданным протоколам взаимодействия и передавать настройки на все точки обеспечения безопасности.

Пример многоагентной системы для организации защиты ПС можно найти в работе [4]. В ней рассматривается использование многоагентных систем для защиты от атак, направленных на отказ в обслуживании (Distributed Denial of Service, DDoS).

Для построения СЗИ на базе МАС каждому компоненту ИС необходимо сопоставить агента, который будет отслеживать изменения в настройках компонента и выполнение им определенных действий, и протоколировать эти операции. Есть два варианта работы агентов. Первый — это сбор данных на основе конфигурационных файлов и файлов аудита. В этом случае система защиты не будет влиять на скорость работы ПС. Однако агенты будут несколько запаздывать, не успевая за изменениями в системе. Второй вариант — реализация обработчиков, которые будут выполняться при определенных событиях в ПС. Например, для Windows такие обработчики называются перехватчиками (англ. hook), а для SQL Server обработчик реализуется с помощью триггеров. Очевидно, что в этом случае код будет «встроен» в саму ПС и будет несколько затормаживать ее основную функциональность. Преимуществом этого варианта является то, что система защиты в режиме реального времени отслеживает изменения в ПС и может сразу на них отреагировать.

На основании собранной информации (состав и количество записей в протоколе) агент может оценить «динамику» компонента, то есть то, как он изменяется в ходе функционирования системы. Непривычные для компонента конфигурации и/или резкое увеличение вызовов определенных операций является подозрительным с точки зрения СЗИ. Для ИС как совокупности компонентов можно говорить о наличии общей динамики системы. Общая динамика — это набор привычных конфигураций компонентов и типичная нагрузка на них. При этом постепенно общая динамика может изменяться, однако резкое отклонение является маловероятным и требует дополнительного анализа.

Изменения можно оценить как качественно, так и количественно. Пример качественного изменения — это отключение межсетевого экрана или включение возможности встроенной аутентификации в SQL Server (помимо Windows-аутентификации). Количественные изменения — это увеличение количества входящих соединений или рост числа пользователей с административными полномочиями. Качественная динамика отображает, что именно произошло, а количественная — сколько раз это произошло. При анализе как качественной, так и количественной динамики можно выявить процесс использования уязвимостей или определить более позднюю фазу атаки, влияющую на конфиденциальность, целостность или доступность информации.

Легче анализировать качественную динамику. Для этого необходимо определить состав операций, выполнение которых является неблагоприятным для ПС, и отслеживать запуск выделенных операций. Для количественной оценки динамики каждой операции необходимо сопоставить некоторую характеристику, которая будет отражать «вклад» операции в динамику компонента, насколько это операция соответствует типичному функционированию или насколько сильно выходит за его рамки. Назовем эту характеристику «коэффициент динамики операции», или КДО. Складывая КДО операций, можно определить динамику отдельного компонента и ИС в целом. Получить эталонные характеристики КДО можно как экспертным путем, то есть с помощью ручного ввода экспертами, так и более универсальным — с помощью этапа обучения для СЗИ.

Одним из возможных способов получения эталонных значений КДО является подсчет количества вызовов операций за время функционирования ИС на этапе обучения. Если за время функционирования ИС T секунд определенная операция была выполнена N раз, то в ходе привычной работы ИС операция должна выполняться не чаще чем $\frac{N}{T}$ раз/с, или $\frac{1}{T/N}$ раз/с. Обратная величина будет показывать, за сколько времени работы ИС ожидается один вызов операции. Чем выше данная величина, тем операция реже вызывалась в ИС и тем непривычнее ее вызов. Чем данная величина ниже, тем привычнее операция для ИС. Эту величину и можно взять за КДО. Развитием описанного способа может быть более глубокий анализ интервалов вызовов операций и связей между этими вызовами.

На этапе обучения агенты будут формировать эталонные значения КДО, которые будут использоваться в «боевом режиме» (на этапе защиты) для выявления атак. За все время функционирования ИС система защиты будет адаптироваться за счет обновления значений эталонных значений. Эксперт по информационной безопасности может в любой момент посмотреть и поправить текущие значения с учетом своего опыта или исходя из планируемых изменений в ИС.

Сигналом опасности будет служить превышение порогового значения разности между эталонными значениями динамики и текущими. Пороговые значения как для отдельного модуля, так и для всей системы могут быть получены на этапе обучения или заданы вручную. Эти характеристики обозначают чувствительность системы защиты к отклонениям в поведении ИС и позволяют (пусть и косвенно) определять требуемый уровень защищенности. При выявлении опасности агент должен оповещать об этом администратора и, возможно, блокировать работу компонента или системы.

Существующие решения для организации адаптивной защиты на базе экспертных систем (ЭС) используют правила, идентифицирующие известные атаки. Эти правила предоставляются администратором, автоматически создаются системой или применяются оба варианта. Правила используются системой для вынесения заключения о состоянии защиты на основе данных, полученных от системы обнаружения атак. Недостатком такого подхода является необходимость частого обновления экспертных систем, иначе ослабляются способности системы защиты, а пользователи вводятся в заблуждение относительно защищенности сети [3]. Еще один недостаток — это плохая адаптация, так как незначительные вариации деталей атаки могут привести к ее пропуску.

В последнее время достаточно активно разрабатываются подходы на основе нейронных сетей. Первоначально нейронная сеть обучается путем правильной идентификации предварительно выбранных объектов предметной области. Реакция нейронной сети анализируется, и система настраивается таким образом, чтобы достичь удовлетворительных результатов. На этапе распознавания достоверность оценки полностью зависит от эффективности этапа обучения. Использование нейронных сетей решает ряд проблем экспертных систем, например необходимость обновления данных, так как нейронные сети автоматически обновляются с течением времени, по мере того как происходит анализ данных. Существуют примеры систем, использующих данный подход для анализа сетевого трафика [3]. Такие системы достаточно сложно обучить, так как для этого необходимо сформировать большое количество атак. Однако в целом подход перспективный, и его можно использовать в рассмотренной выше архитектуре адаптивной СЗИ для анализа отклонений в работе ИС. Для этого на этапе обучения агент будет настраиваться на распознавание класса «типичных» для модуля состояний, за счет чего на этапе функционирования системы защиты агент сможет выявлять аномальные состояния модуля — те, которые не попали в класс «типичных». Выявленные события будут образовывать новый класс состояний, о которых необходимо сигнализировать персоналу, ответственному за безопасность.

Предлагаемый метод построения адаптивных систем защиты позволяет задействовать преимущества многоагентных систем, такие как масштабируемость, экономичность, отказоустойчивость и др. Использование в работе системы защиты динамически определяемых КДО придает системе возможность легкой адаптации к новым видам атак. За счет этого решается ряд проблем существующих систем, в основе которых лежат ЭС, — необходимость частого обновления баз сигнатур и слабая возможность адаптации. Указанная возможность интеграции в СЗИ нейронных сетей для анализа отклонений является дополнительным потенциалом для адаптации. Предложенный подход предполагается взять за основу для построения максимально гибкой адаптивной системы защиты в соответствии со структурой сети, требуемым уровнем безопасности и имеющимися вычислительными ресурсами.

СПИСОК ЛИТЕРАТУРЫ:

1. *Когаловский М. Р.* Перспективные технологии информационных систем. М.: ДМК-Пресс, 2003. – 288 с.
2. *Галатенко В. А.* Основы информационной безопасности. ИНТУИТ.ру, 2008. – 208 с.
3. *Крыжановский А. В.* Применение искусственных нейронных сетей в системах обнаружения атак // Доклады Томского государственного университета систем управления и радиоэлектроники. Томск: Томский государственный университет систем управления и радиоэлектроники, 2008. Т. 2. С. 104–105.
4. *Котенко И. В., Уланов А. В.* Кооперативная работа команд агентов при защите от сетевых атак нарушения доступности // Труды Международных научно-технических конференций «Интеллектуальные системы (AIS'06)» и «Интеллектуальные САПР (CAD-2006)». М.: Физматлит, 2006. С. 306–313.