2 Забазпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 004.4

ТАКСОНОМИЯ, ТЕНДЕНЦИИ РАЗВИТИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Александр Голяка
НБУ

Аннотация: **Представлен обзор и классификация систем обнаружения вторжений.**
Summary: **A review and classification of intrusion detection systems.**
Ключевые слова: **Системы обнаружения вторжений, IDS датчики, IPS датчики, RBID и SBID системы.**

В условиях современного развития информационных технологий в дополнение к общепринятым средствам защиты информации, основанным на разграничении и контроле прав доступа, авторизации и криптозащите данных, межсетевых экранах (МСЭ) все чаще используют системы обнаружения вторжений (intrusion detection systems – IDS) (СОВ). Угрозы и риски, связанные с компьютерными сетями предприятий, многочисленны и возникают не только за периметром сети, но и внутри организации, как преднамеренно, так и случайно. Эффективные системы по наблюдению за безопасностью учитывают максимально возможные риски и требуют глубокого понимания этих рисков, текущей архитектуры сети предприятия, признаки потенциальных угроз и действий, которые могут подвергнуть опасности данные, размещенные на компьютерах этой сети.

В информационно-телекоммуникационной системе (ИТС) СОВ осуществляет защиту практически от тех же угроз, что и межсетевой экран, однако между ними есть принципиальные различия. В то время как МСЭ главным образом фильтрует нежелательный входящий/исходящий трафик системы, СОВ анализирует определенные параметры системы, в том числе и трафик, и может сигнализировать о вторжении в ИТС. Поэтому МСЭ и СОВ обычно работают совместно, и атаки, которые МСЭ пропускает, обнаруживает СОВ. Кроме того, обнаружив атаку, СОВ может переконфигурировать МСЭ для того, чтобы нейтрализовать эту атаку. Некоторые специалисты выделяют системы с возможностью реакции на атаку как отдельный класс, называя такие системы IPS (система предотвращения/защиты от вторжений). В этом случае СОВ – это системы, которые только осуществляют мониторинг с ответными действиями после атаки (разрыв TCP или блокировка на внешнем устройстве), а функциональность IPS – это линейный мониторинг с возможностью «отклонения пакета» (которая, однако, не обязательно используется). Тогда вводят еще третий термин IDP – система выявления и предотвращения вторжений, объединяющий IDS и IPS. В данной статье под СОВ будем понимать IDP (рис. 1).

Основным преимуществом СОВ является предотвращение так называемых инсайдерских атак – вторжений изнутри организации. Как показывает практика, атаки на ресурсы, организованные пользователями, имеющими определенные права доступа в ИТС, становятся все более распространенными и значительными.

Концепция обнаружения вторжений для компьютерных систем была разработана в конце 80-х годов. Американским Департаментом Защиты (DOD) было проанализировано несколько моделей для отслеживания и анализа различных типов атак. Концепция, разработанная первоначально, называлась Распределенные системы по обнаружению вторжений (DIDS – Distributed Intrusion Detection Systems). Эти системы использовали популярные методы по обнаружению вторжений – анализ веб-журналов, журналов аудита маршрутизаторов и любой другой необычной сетевой активности.

Под вторжением в компьютерную систему будем понимать любую деятельность, которая нарушает целостность, конфиденциальность или доступность данных системы. В качестве целей атак могут выступать сервера, рабочие станции пользователей или коммуникационное оборудование ИТС. Обнаружение вторжений – это процесс идентификации подозрительной деятельности, направленной на вычислительные или сетевые ресурсы, и своевременного реагирования на нее. Основным источником информации для СОВ являются всевозможные системные журналы и протоколы: содержание сетевого трафика; показатели функционирования системы, такие как число операций ввода-вывода, количество работающих процессов;

информация о производительности программно-аппаратного обеспечения, например, объем используемой памяти и т. д.; информация о работе пользователей с файлами и другими ресурсами системы; административная деятельность, например, регистрация новых пользователей.

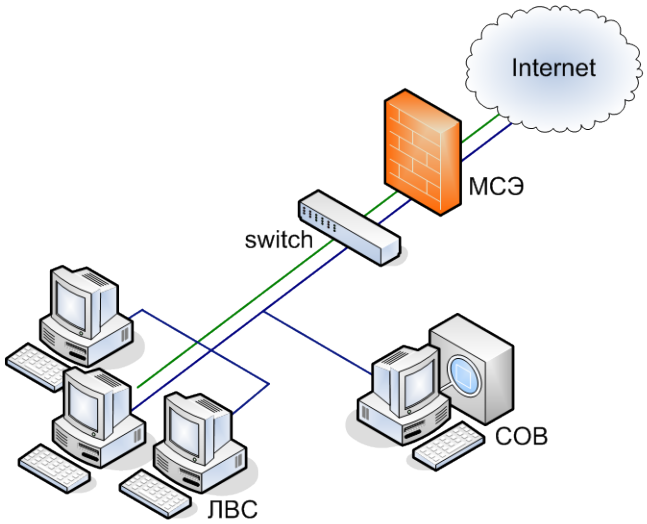

Рисунок 1 – Схема размещения СОВ

Сбор исходных данных осуществляется при помощи специализированных датчиков, размещаемых в ИТС, это одни из самых важных элементов СОВ. СОВ может включать в себя два типа датчиков – сетевые и компьютерные. Сетевые датчики предназначены для сбора информации о пакетах данных, передаваемых в том сегменте ИТС, где установлен датчик. Вторые устанавливаются на определённые компьютеры в ИТС и предназначаются для сбора информации о событиях, возникающих на этих компьютерах. При этом на одном узле может присутствовать одновременно несколько компьютерных датчиков, предназначенных для сбора различной информации. Обычно вся полученная датчиками информация поступает на узел обработки информации и принятия решений.

Сетевые датчики бывают 2-х видов. 1-й тип показан на рис. 2.

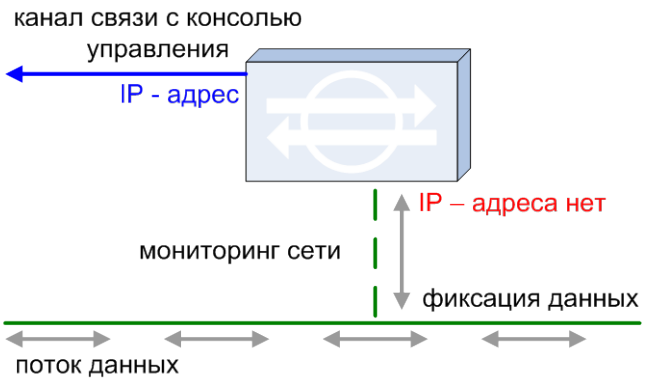

Рисунок 2 – Сетевой датчик 1-го типа

Обычно, при качественной реализации, этот тип датчика имеет следующие функции и возможности:

- мониторинг трафика в заданном сегменте: фиксация SPAN, TAP, VACL и т. д.;
- сопоставление трафика с сигнатурами атак; поиск эвристических шаблонов атаки, аномалий протоколов;
- определение характера атак на основе встроенных логических алгоритмов фрагментации и повторной сборки потока;

- инструмент выдачи сигналов тревоги и наглядного представления, но также предоставляется возможность для определенных активных действий: разрыв TCP, блокирование, регистрация сеанса IP.

Такие датчики называют IDS датчиками.

2-й тип датчиков показан на рис. 3.

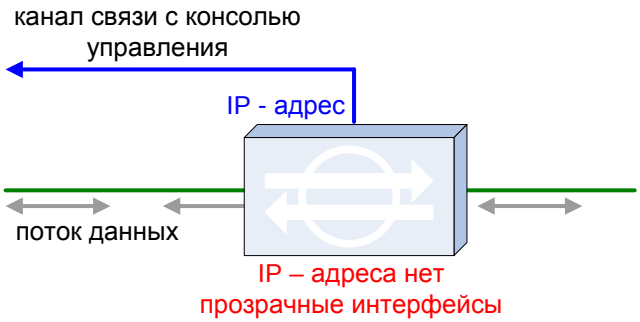

Рисунок 3 – Сетевой датчик 2-го типа

Этот тип датчика обычно имеет следующие функции и возможности:

- выполняет мониторинг всего трафика, «прозрачно» проходящего двумя интерфейсами;
- сопоставляет трафик с хорошо известными сигнатурами атак, также осуществляет поиск эвристических шаблонов атак и аномалий протоколов;
- включает логический алгоритм фрагментации для четкого определения характера атак, а также нормализации потока пакетов TCP/IP;
- служит одновременно инструментом выдачи сигналов тревоги и наглядного представления, выполняет задачи профилактики путем фильтрации пакетов. Кроме того, обеспечивает возможность активных ответных действий: разрыв TCP, блокировка, регистрация сеанса IP и отклонение пакета/потока/пользователя.

Такие датчики называют IPS датчиками.

Кроме описанных основных преимуществ и функций, СОВ может также решать следующие задачи.

1. Очень часто злоумышленники выводят из строя межсетевые экраны с целью дальнейшего бесконтрольного проникновения в корпоративную сеть. Чтобы снизить вероятность такого проникновения можно использовать системы обнаружения атак, функционирующие на уровне сети, для временного резервирования функций межсетевого экрана. СОВ позволяют осуществить фильтрацию сетевого трафика по различным полям заголовка IP-пакета, что позволяет организовать достаточно мощный пакетный фильтр, мало чем уступающий возможностям настоящего межсетевого экрана.

Кроме того, СОВ могут использоваться для временного замещения межсетевого экрана во время регламентных работ по обновлению программного обеспечения МСЭ или тестирования его настроек.

2. Контроль доступа к файлам. При этом могут быть использованы как системы, анализирующие журналы регистрации (например, RealSecure Server Sensor), так и анализирующие системные вызовы (например, Entercept).

3. Нередки случаи, когда сотрудники компании используют служебный доступ в Internet в своих личных целях – для поиска работы, рассылки резюме, спама и других несанкционированных действий. Все это приводит к потере производительности труда, увеличению расходов на оплату услуг Internet и т. д. Часто происходит утечка конфиденциальной служебной информации, которая может происходить не только по электронной почте, но и при обращении к какому-либо внешнему Web-серверу. С целью предотвращения таких действий и обнаружения неблагонадежных сотрудников могут применяться СОВ.

4. Антивирусная защита. СОВ могут быть применены и в данном случае. И хотя они в полном объеме не смогут заменить классическую антивирусную систему, но частично могут блокировать проникновение вирусов и троянских коней в корпоративную сеть.

5. Системы обнаружения вторжений, функционирующие как на уровне сети, так и на уровне конкретного узла, могут быть использованы для контроля несанкционированных изменений конфигурации защищаемых узлов со стороны пользователей, обладающих административными привилегиями. В данном случае эти системы выступают в качестве дополнительного средства контроля.

6. Нередки случаи, когда злоумышленники подключают свои компьютеры или notebook'и к критичным сегментам сети с целью получения доступа к передаваемой конфиденциальной информации (например,

паролям или платежным поручениям). Установленные на таких компьютерах анализаторы протоколов (снифферы) позволяют перехватывать весь сетевой трафик, циркулирующий между узлами критичного сегмента. Опасность таких несанкционированно подключенных устройств в том, что они без труда получают доступ к паролям пользователей (в т. ч. и администратора), передаваемых в незащищенном виде по большинству протоколов, построенных на базе стека TCP/IP. В частности, беззащитными в данном случае являются протоколы: HTTP, FTP, Telnet, POP3, IMAP и т. д. В т. ч. открытой остается и информация, передаваемая между SQL-сервером и клиентским программным обеспечением.

Нередко сотрудники компаний, в которых доступ в Internet регламентируется и разграничивается с помощью различных защитных средств (например, межсетевых экранов или систем контроля содержания), подключают к своим компьютерам модемы и используют их для выхода в Internet в обход защитных механизмов. Также модемы очень часто используются для получения обновлений различных юридических и бухгалтерских программ. И, наконец, модемы могут быть использованы для доступа к рабочему месту из дома. Это представляет большую угрозу для многих компаний, т. к. компьютеры, к которым подключены модемы, никак не защищены и любой злоумышленник, обнаруживший такой "черный ход", может воспользоваться им для несанкционированного доступа к ресурсам, требующим обязательной защиты.

СОВ позволяют обнаруживать в контролируемых сегментах сети посторонние адреса от "чужих" компьютеров и узлов, а также по непонятной причине возросший трафик от какой-либо рабочей станции, ранее не замеченной в такой активности, что может свидетельствовать о работе с этого узла злоумышленника, проникшего на него через модем.

7. Межсетевой экран – необходимое средство для защиты информационных ресурсов корпоративной сети. Но обеспечить необходимый уровень сетевой безопасности можно только при правильной настройке межсетевого экрана.

Установка сетевых датчиков СОВ до и после межсетевого экрана позволяет проверить эффективность его настроек за счет сравнения числа атак, обнаруженных до и после МСЭ.

8. Нередки ситуация, когда сотрудники отделов защиты информации и отделов телекоммуникаций не владеют достоверной информацией об используемых в защищаемых сегментах сети протоколах. С помощью СОВ можно контролировать все используемые в сети протоколы и сервисы, а также частоту их использования, что позволяет построить схему информационных потоков в организации и карту сети, являющуюся залогом успешного создания инфраструктуры защиты информации в организации.

9. Журналы регистрации маршрутизаторов и иных сетевых устройств являются дополнительным источником информации об атаках, направленных на информационные ресурсы корпоративной сети. Однако эти журналы регистрации обычно не анализируются на предмет обнаружения в них следов несанкционированной деятельности, т. к. практически отсутствуют или очень дорого стоят средства (например, netForensics), решающие эту задачу.

Функция сбора журналов регистрации и анализа событий в них может быть возложена на СОВ, выступающую в качестве Syslog-сервера, которая сможет не только осуществить централизованный сбор, но и обнаружение атак и злоупотреблений в этих журналах. Кроме того, это дополнительная мера защиты журналов регистрации от несанкционированного изменения, т. к. события, фиксируемые маршрутизаторами, сразу же передаются на сенсор СОВ, что не позволяет злоумышленнику удалить или изменить компрометирующие его следы.

10. СОВ могут и должны быть использованы для сбора доказательств несанкционированной деятельности за счет следующих возможностей:

- запись событий, происходящих во время атаки, для дальнейшего анализа и исследований;
- имитация несуществующих приложений с целью введения злоумышленника в заблуждение (т. н. режим обманной системы);
- расширенный анализ журналов регистрации прикладных и системных приложений, серверов баз данных, Web-серверов и т. д.;
- возможность исследования событий безопасности перед выполнением каких-либо действий;
- получение DNS-, MAC-, NetBIOS- и IP-адресов компьютера злоумышленника.

Классификация СОВ

Существует несколько видов классификации СОВ.

По способу сбора информации об атаке СОВ делятся на network-based, host-based, application-based. Т. е., в зависимости от того, где осуществляется сбор информации: в сети, на конкретном компьютере или на конкретных приложениях, работающих на компьютере. Соответственно, возможна комбинация перечисленных методов сбора информации.

По способу анализа данных СОВ делятся на две группы – signature-based (RBID) и anomaly-based (SBID). Т. е. сигнатурные и поведенческие.

Традиционны и наиболее развиты СОВ первого типа. Они представляют каждую атаку в виде специальной модели или «сигнатуры», описывающие характеристики и сценарии возможных атак. RBID системы анализируют полученную с датчиков информацию и сравнивают результаты с предустановленной базой сигнатур атак, и в случае совпадений фиксируется факт атаки. Сигнатуры весьма разнообразны и могут определять некие параметры от номера порта в пакете до последовательности байт в серии пакетов, количество попыток ввода пароля и т. д. Сигнатуры могут представлять собой строку символов, семантическое выражение на специальном языке и т. д. Использование разработанной сигнатуры позволяет обычно довольно эффективно обнаруживать подозрительную сетевую активность. В настоящее время перспективными считаются 3 метода сигнатурного анализа. Метод контекстного поиска, позволяющий наиболее точно задать параметры сигнатуры, которую необходимо выявить в потоке исходных данных, метод анализа состояний и метод, базирующийся на экспертных системах. Метод анализа состояний формирует сигнатуры атак в виде последовательности переходов ИТС из одного состояния в другое. При этом каждый такой переход связан с наступлением в ИТС определённых событий, которые определяются в параметрах сигнатуры атаки. Такие сигнатуры атак обычно описываются при помощи математических аппаратов конечных автоматов или сетей Петри. Методы выявления атак, базирующиеся на экспертных системах, позволяют описывать модели атак на высоко абстрактном естественном языке. Такая экспертная система состоит из базы фактов и базы правил. Факты представляют собой исходные данные о работе ИТС, а правила – методы логического вывода об атаке на основе имеющейся базы фактов. Правила описывают характерные признаки атак, которые должна обнаруживать СОВ.

Достоинства RBID систем:

- довольно четкое определение типа атаки, высокая точность работы практически без ложных срабатываний.

Недостатки:

- неустойчивость к новейшим типам атак, поскольку на момент атаки базы знаний (сигнатур) еще не содержат соответствующих сценариев;
- зависимость эффективности работы от скорости разработки новых сигнатур атак;
- происходит потеря времени от разработки сигнатуры разработчиками СОВ до обновления базы данных сигнатур организацией потребителя СОВ;
- для сложных распределенных атак проверка на соответствие сигнатуре является нетривиальной задачей;
- большинство баз знаний сигнатур и правил общедоступны, поэтому нарушитель может использовать методы «маскировки» атаки.

Большинство этих недостатков можно свести к минимальному влиянию на успешность СОВ, но главная проблема остается всегда – если атака новая и для нее нет сигнатуры, то обнаружена она вероятно не будет.

Второй тип СОВ – SBID основан на контроле частоты событий или обнаружении статистических аномалий. Такие системы больше ориентированы на выявление новых типов атак. SBID за определенное время работы (период обучения) вычисляет «нормальную» сетевую активность и затем в эксплуатационном режиме анализирует параметры работы сети, и то, что не попадает под определение «нормально», помечается как аномалия. Аномалию можно рассматривать с трех позиций: аномалия протокола (включает в себя поиск отклонений от стандартного протокола), аномалия сети (включает в себя наблюдение или запоминание нормальных уровней трафика), поведенческая аномалия (включает в себя запоминание нормального поведения пользователя). Наиболее эффективна против ложных тревог СОВ комбинация этих позиций наблюдения аномалий.

Особенностью любой SBID системы является её возможность изучать сетевую активность и отличать нормальную сетевую активность от аномальной. Наиболее часто SBID реализуются на основе статистических моделей. Эти модели определяют статистические показатели, которые характеризуют параметры штатного поведения системы. Если при работе ИТС эти параметры отклоняются от своих заданных значений, то метод позволяет сделать вывод о факте реализации атаки. В качестве таких параметров могут выступать: уровень загруженности процессора, загрузка каналов связи ИТС, штатное время работы пользователей системы, количество обращений пользователей к сетевым ресурсам ИТС и т. д. Существует множество статистических моделей. Наиболее применимы три из них:

- пороговая модель, которая для каждого статистического параметра определяет пороговые величины; если наблюдаемый параметр превышает заданный порог, то это событие является признаком потенциальной атаки;

• модель среднего значения и среднеквадратичного отклонения, которая для каждого статистического параметра определяет так называемый доверенный интервал на основе математического ожидания и дисперсии; если текущее значение параметра не укладывается в этом интервале, то случай рассматривается как атака;

• многовариационная модель, которая аналогична модели среднего значения и среднеквадратичного отклонения, но позволяет одновременно учитывать корреляцию между большим количеством статистических показателей.

Достоинства SBID систем:

• могут обнаруживать совершенно новые виды атак;

• способны обнаружить атаки, характеризующиеся большой продолжительностью во времени;

• такие системы в некотором смысле проще обслуживать, так как нет нужды в обновлении сигнатур.

Недостатки:

• сложно построить модель «нормальной» работы сети, поэтому SBID склонны к ложному срабатыванию сигналов об атаках;

• такие системы необходимо «обучать» некоторый период времени и они не могут работать сразу же после инсталляции в ИТС;

• введением такой системы в эксплуатацию должны заниматься высококвалифицированные в данном направлении специалисты;

• в отличие от RBID систем, SBID не генерируют сообщения, точно описывающие атаку; при атаке будет сгенерировано только сообщение об «аномальности», возможно с некоторой дополнительной информацией и статистическими характеристиками;

• необходимость установки эффективного порогового значения для сигнализации атаки; это окажет влияние либо на увеличение частоты ложных срабатываний, либо система не будет выдавать сигналы там, где необходимо.

В связи с недостатками обоих принципов построения СОВ в последнее время специалисты склоны дополнять работу проверенных и давно работающих RBID систем SBID системами (получаются так называемые многоуровневые системы). Тогда СОВ, основанные на правилах (сигнатурах) обнаруживают известные атаки, в то время как статистические СОВ могут отлавливать неизвестные базе сигнатур случаи.

В заключение можно утверждать следующее. В самом общем случае главной задачей развития средств, реализующих технологии обнаружения атак, является автоматизация рутинных функций по обеспечению информационной безопасности корпоративной сети и преобразование этих функций в посильные для персонала, не являющегося экспертами в области защиты информации.

Тенденции на рынке СОВ состоят в объединении различных методик обнаружения несанкционированной активности – сигнатур, аномалий протоколов, контроля поведения трафика и т. д.; интеграции с сетевым оборудованием, переходом на программно-аппаратные решения, постепенном отказе от сигнатурных методов в пользу поведенческих. Учитывая также, что вредоносные программы в последнее время все сложнее классифицировать, можно прогнозировать, что в будущем классы антивирусного ПО и СОВ сольются. Уже сейчас в описании многих антивирусов встречаются фразы «обнаруживает компьютерные атаки». В свою очередь в документации на СОВ встречаются «идентифицирует сетевые вирусы, троянцы и черви».

Література: ***1.*** *Лукацкий А. В. Обнаружение атак. 2-е издание. БХВ-Петербург, 2003., 569 с.* ***2.*** *Mukherjee, B., Heberlein, L. T., and Levitt, K. N. (1994). Network intrusion detection. IEEE Network, 26–41.* ***3.*** *Porras, P. A., Ilgun, K., and Kemmerer, R. A. (1995). State transition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering,SE-21: 181–199.* ***4.*** *Denning, D. E. (1987). An intrusion detection model. IEEE Transactions on Software Engineering, SE-13:222–232.* ***5.*** *Edward Amoroso. Intrusion Detection. An Introduction to Internet. Surveillance, Correlation, Trace Back, Traps and Response. – Intrusion.Net Books, 1999.*