В. С. Веденеев, И. В. Бычков

СРЕДСТВА ПОИСКА ИНСАЙДЕРОВ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Введение

Поиск внутреннего нарушителя информационной безопасности (ИБ) является одним из приоритетных направлений в работе служб безопасности организаций. Внутренний нарушитель обладает сведениями о работе компьютерной системы (КС), вероятнее всего знаком с сотрудниками, обслуживающими и администрирующими КС, имеет ряд разрешений на доступ к внутренней информации, может знать парольную информацию коллег, обладает физическим доступом к некоторым компьютерам. Кроме того, внутренний нарушитель менее ограничен в действиях средствами защиты информации в отличие от внешнего нарушителя.

Видами вредоносных действий инсайдеров являются [1]: кража интеллектуальной собственности, ИТ-саботаж, мошенничество (кража конфиденциальных данных), шпионаж и случайное непреднамеренное действие.

Особенность выявления инсайдеров состоит в том, что, как правило, их действия не направлены на преодоление средств или систем защиты информации. Инсайдеры действуют в рамках данных им полномочий и используют имеющиеся у них знания и информацию о КС для нанесения ущерба.

В настоящей работе рассмотрены основные средства поиска внутренних нарушителей, предоставляющие исходные данные для специалистов по информационной безопасности. Также эти данные могут обрабатываться математическими алгоритмами в специальных программах для выявления скрытых закономерностей в действиях пользователей.

1. Data leakage protection (DLP-системы)

На настоящий момент существует достаточно большое число dlp-систем (data leakage protection — система предотвращения утечек информации) или им подобных программ, позволяющих выявлять утечки конфиденциальной информации и нелояльных сотрудников.

DLP-системы основываются на перехвате информации, передаваемой пользователем по компьютерной сети и на периферийные устройства (принтеры, USB-носители и др.). В отдельных случаях система может контролировать работу самого пользователя — осуществлять перехват клавиатуры, снимков экрана и др.

Выделяются несколько типов DLP-систем.

Первый — шлюзовые DLP-системы, которые устанавливаются на центральных узлах локальной сети. При таком подключении DLP-система остается скрытной от пользователей КС. Информация на сервер DLP-системы поступает либо с зеркалируемого коммутатора (или специально настроенного маршрутизатора), либо непосредственно, программно с сервиса КС (агент DLP-системы устанавливается на один сервер с сервисом КС, например с прокси-сервером, и передает информацию на DLP-сервер).

Второй тип DLP-систем — хостовые системы, то есть системы, устанавливаемые непосредственно на ПК пользователя.

Комбинированные системы используют оба типа установок. На сегодняшний день комбинированные системы получили наибольшее распространение.

Существует несколько видов обработки перехваченной и приведенной к общему формату информации. Цель обработки — среди потока данных найти вхождения конфиденциальной информации.

Основные используемые алгоритмы:

1. Поиск по регулярным выражениям (перехват данных определенного формата, например номер паспорта, ФИО и т. д.).

2. Поиск подобных (цифровые отпечатки и т. п.) — поиск определенных шаблонов в документах.

3. Сигнатурный анализ (поиск вхождений текста).

4. Лингвистический поиск (поиск с учетом особенностей языка и языковых выражений).

5. Распознавание текста из изображений и последующий анализ и др.

В дальнейшем может проводиться ручной поиск данных среди информации, выделенной в так называемый «карантин».

Однако угрозы целостности и доступности конфиденциальной информации такими системами не предотвращаются. Кроме того, использование DLP-систем ограничено на законодательном уровне (тайна переписки, тайна личной жизни и др.), и при внедрении DLP следует получить юридическую консультацию и провести ряд организационных мер.

2. Honeypot

К средствам обнаружения нарушителя относятся системы «honeypot» (пер. с англ. — «горшочек с медом») [2, 3, 4]. Honeypot представляет собой муляж какой-либо части КС, например СУБД, сетевого сервиса или выделенного сервера. Honeypot не выполняет никакой полезной работы и должен быть неизвестен пользователям КС. Основная цель honeypot — привлечь внимание нарушителя. Honeypot срабатывает и сигнализирует администратору системы об обследовании или попытке взлома муляжа. Honeypot может реализовываться как на отдельном физическом сервере, так и в виртуальной среде.

К достоинствам honeypot относятся [2]: малое число ложных срабатываний (любое обращение к honeypot уже является тревожным знаком), уменьшение по сравнению с «традиционными» средствами защиты информации количества ложных срабатываний, перехват неизвестных ранее атак, большая гибкость, что позволяет адаптировать honeypot к любой КС, минимальное количество программно-аппаратных ресурсов даже для большой КС.

Honeynet представляет собой объединение двух и более физических (не виртуальных) honeypot в одну сеть. Одним из требований построения honeynet является сходство элементов honeynet с узлами, используемыми в КС: базами данных, веб-серверами и т. п. Все обращения к элементам honeynet фиксируются и исследуются специалистами. Таким образом, honeynet позволяет исследовать действия, приемы и тактику нарушителя.

Кроме honeypot используются и так называемые honeytoken. Honeytoken, в отличие от honeypot, не предполагает наличие аппаратной части [5]. Honeytoken представляет собой своеобразную приманку: информацию, которая может заинтересовать злоумышленника. При этом в действительности она не является ценной для организации. [6] Информация представляется в виде файла, записи в базе данных, пары логин/пароль таким образом, чтобы перемещение honeytoken можно было отслеживать. К honeytoken создается свободный доступ. Отслеживание перемещений производится при помощи меток, перехватываемых системами обнаружения вторжений. О каждом перемещении оповещается администратор безопасности.

3. Security Information and Event Management

SIEM-системы (англ. Security Information and Event Management) — системы, состоящие из агентов, устанавливаемых на различных частях КС, сборщиков информации от агентов, механизма, приводящего данные к единой форме, и механизма, анализирующего полученные от агентов данные. SIEM-система используется при управлении рисками ИБ, выявлении нарушения ИБ,

анализе и разборе произошедшего инцидента ИБ, создании рекомендаций по противодействию нарушителям в случае обнаружения угрозы ИБ.

Основная задача SIEM-системы — фиксировать события, происходящие в КС, и сигнализировать сотруднику службы ИБ о событиях, предшествующих атаке на КС.

В SIEM-системах используется большое число различных математических алгоритмов для обработки и анализа полученных событий [7].

SIEM-система способна выявлять:

- известную и описанную правилами угрозу,
- типовую угрозу,
- аномальное поведение пользователей,
- отклонения от жестко заданных правил работы в КС,
- причинно-следственную связь между событиями (при использовании алгоритмов корреляции на основе графов, статистических методов, байесовской вероятности [7]).

Даже без использования специальных алгоритмов некоторые события, перехваченные SIEM-системой, могут напрямую сигнализировать об инсайдерской атаке. Например: подключение к КС через VPN во внерабочее время, увеличение сетевой активности и др. Более подробно о настройка SIEM-систем для обнаружения инсайдерских атак описана в работе [8].

4. Программы tripwire

Одним из способов выявления нарушителя являются программы tripwire (пер. с англ. — «заграждение», «натянутая проволока»), которые отслеживают изменения в конфигурационных и других файлах и оповещают об этом администратора КС. При первом запуске система вычисляет хэш-функции от важных файлов КС и далее с заданным администратором периодом отслеживает изменения в файлах.

5. Типовые способы применения

В зависимости от направления вредоносной деятельности инсайдеров применяются следующие комплексы средств и систем:

1. Кража интеллектуальной собственности:

- DLP-система — контроль периферийных устройств: вывод документов на печать, на внешние носители, на сетевые средства, например Bluetooth, и др.;

- SIEM-система фиксирует аномальную активность пользователя, например: увеличение числа обращений к определенным документам, числа документов, отправляемых на печать, по электронной почте, попытки подбора паролей и др.

2. ИТ-саботаж:

- SIEM-система: наиболее вероятным действием нарушителя в таком случае является создание backdoor'ов и логических бомб. SIEM-система, благодаря встроенным алгоритмам графов атак, сигнатурным правилам и правилам корреляции, заданным согласно политике ИБ, способна выявлять подобные угрозы;

- программы tripwire оповещают об изменении системных файлов, которое может оставаться незамеченным длительное время до перезагрузки сервиса или сервера.

3. Мошенничество, кража данных: аналогично п. 1, но при этом DLP-система должна быть настроена на перехват специфических видов данных, например финансовых данных, персональных данных и т. п.

4. Шпионаж:

- honeypot, honeytoken — при активном поиске конфиденциальных данных злоумышленник может найти, например, файл со специально подготовленной парой логин-пароль, вымышленными

персональными данными, вымышленной служебной информацией. Любое использование такого файла расценивается как инсайдерская деятельность;

- **DLP-система**: результаты шпионажа могут быть отправлены средствами корпоративной КС;
- **SIEM-система**: выявление аномалий в работе пользователей — увеличений числа обращений к определенным документам, увеличений объемов, передаваемых по Сети.

5. Случайное, непреднамеренное действие:

- **SIEM-система**: выявление отклонений от заданных режимов работы;
- **DLP-системы** выявляют передачу конфиденциальных данных, отправленных по ошибке.

Сформулируем несколько рекомендаций по использованию данных средств. Прежде всего, рассмотрим компании — разработчики ПО, для которых актуальными угрозами являются кража интеллектуальной собственности (программного кода) и саботаж — внедрение логической бомбы в код программ. Рекомендуемый набор средств будет следующим. Во-первых, использование системы контроля версий (SVN, Git и др., распространяющиеся по открытой лицензии) для постоянного контроля изменений в коде программ. Кроме того, использование системы контроля версий позволит значительно оптимизировать процесс разработки. Во-вторых, внедрение DLP-системы для предотвращения переноса кода на внешние носители и в сеть Интернет. Стоимость DLP-систем обычно открыто не объявляется. Исключением является комплекс «Контур безопасности» компании SearchInform, стоимость которого можно рассчитать на сайте компании.

Для банков наиболее подходящими средствами для предотвращения внутренней угрозы являются DLP-системы, способные, в том числе, выявить аномальное поведение пользователей, установку в локальной сети honeypot и honeynet. Актуальным представляется вопрос о внедрении SIEM-системы для обработки всех событий ИБ.

В общем случае SIEM-системы из-за большой стоимости подходят большим распределенным компаниям (более 1000 ПК и множество средств защиты информации).

Для малых и средних коммерческих структур оптимальным средством для предотвращения инсайдерских угроз является внедрение DLP-систем, а также периодический ненавязчивый контроль за действиями сотрудников как способ выявления аномального поведения. К примеру, периодическая визуальная проверка данных, введенных в ERP-систему.

Кроме того, не следует забывать, что средства обнаружения инсайдеров должны применяться в комплексе с остальными средствами защиты информации: средствами антивирусной защиты, межсетевого экранирования и др.

Заключение

В работе рассмотрены основные средства и системы, позволяющие выявлять все основные виды инсайдерских атак в корпоративных информационных системах. Эффективность указанных выше систем напрямую зависит от согласованности их архитектуры и настроек с особенностями частных КС. Так, DLP-система помимо базовых настроек должна иметь настройку на перехват специфических именно для конкретной КС данных. Сенсоры SIEM-системы должны быть расположены таким образом, чтобы поставляемые ими данные обеспечивали наиболее полную информацию о происходящих в КС событиях.

Можно выделить два главных вектора развития: во-первых, совершенствование существующих средств и систем выявления инсайдеров, совершенствование алгоритмов их работы; во-вторых, создание комплексных алгоритмов и адаптация методов Data Mining для обработки событий компьютерной системы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Silowash G., Cappelli D., Moore A., Trzeciak R., Shimeall T., Flynn L.* (2012). Common Sense Guide to Mitigating Insider Threats. 4th edition. (CMU/SEI-2012-TR-012) Software Engineering Institute. Carnegie Mellon University Website. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017 (дата обращения: 17.03.2014г.).
2. *Spitzner L.* Honeypots: Catching the Insider Threat // Computer-Security Application Conference, 2003. Proceesings, 19th Annual. 2003. P. 170–179.
3. *Even L. R.* Intrusion Detection FAQ: What is a Honeypot? 2000.URL: http://www.sans.org/security-resources/idfaq/honeypot3.php (дата обращения: 17.03.2014г.).
4. Honeypot (computing) // Wikipedia, the free encyclopedia. URL: http://en.wikipedia.org/wiki/Honeypot_(computing) (дата обращения: 18.03.2014г.).
5. Honeytoken // Wikipedia, the free encyclopedia. URL: http://en.wikipedia.org/wiki/Honeytoken (дата обращения: 16.03.2014г.).
6. *Maybury M., Chase P., Cheikes B., Brackney D., Matzner S., Hetherington T., Wood B., Sibley C., Marin J., Longstaff T., et al.* Analysis and Detection of Malicious Insiders // International Conference of Intelligence Analysis. McLean. VA. 2005.
7. *Шелестова О.* SIEM и (или) сканер уязвимостей // Positive Research. 2012. URL: http://blog.ptsecurity.ru/2012/10/siem_1.html (дата обращения: 17.03.2014г.).
8. Using a SIEM signature to detect potentional precursor to IT Sabotage. CERT Insider Threat Center, Insider Threat Control, 2011. URL: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=69381 (дата обращения: 16.03.2014г.).