Предсказание и обнаружение инсайдерских атак

Санжапова Юнна Алиевна,
студентка МГТУ им. Н. Э. Баумана

Ни для кого не секрет, что порой даже самый близкий человек может причинить большее зло, чем заклятый враг. Эта истина верна и в области информационной безопасности. Вы спросите, почему? За ответом обратимся к красноречивой статистике: материальные убытки организаций, подверженных аутсайдерским атакам, составляют 60 000 долларов, в то время как потери, вызванные инсайдерскими атаками, превысили 2,7 млн долларов. Разница в 45 раз — это серьезный повод задуматься. Реализованные инсайдерские атаки могут в одночасье довести успешно развивающую компанию до состояния банкрота, так как часто объектом внимания злоумышленников становятся исходные тексты компьютерных программ или другая секретная информация. Но — обо всём по порядку.

Инсайдерские атаки — одна из наименее изученных и незаслуженно недооцененных угроз безопасности, которые стоят перед организациями в наши дни. Тот факт, что термин «инсайдер» у всех на слуху и не имеет конкретного толкования, делает эту проблему и ее многочисленные стороны ещё более сложными для понимания. Хотя сотрудники организации, несомненно, являются потенциальными инсайдерами, относятся ли к инсайдерам консультанты, клиенты, подрядчики, поставщики, партнеры по бизнесу и т.д.— вопрос неоднозначный. Существует распространенное мнение, что любое лицо, которое имеет доступ к вычислительным ресурсам организации, а следовательно, обладает логином и паролем,— это инсайдер. Если данное определение понимать буквально, то инсайдерами можно считать пользователей, имеющих доступ к подписному веб-сайту, даже если они никогда не работали на организацию, обслуживающую данный веб-сайт.

Что касается мнения зарубежных специалистов в области компьютерной безопасности, то Т. Тугулар (T. Tugular) и Е. Спаффорд (E. H. Spafford) относят к инсайдерам пользователей автоматизированной системы, имеющих доступ к её ресурсам на назначенном уровне привилегий, но использующих систему в обход правил разграничения доступа, тем самым нарушая политику информационной безопасности организации. Специалист Н. Айнвахтер (N. Einwechter) даёт следующее определение термина «инсайдер»: это легальный пользователь, который вместо исполнения возложенных на него обязанностей нарушает правила разграничения доступа, чтобы использовать систему в своих целях.

Выше было сказано, что объектом манипуляций инсайдеров является информация. Инсайдер может нарушить одно, два или даже все три основных свойства информации — КЦД: конфиденциальность, целостность, доступность. Примером нарушения конфиденциальности может служить раскрытие персональных данных, целостности — несанкционированное изменение данных организации, доступности — уничтожение информационной собственности организации (при этом одновременно нарушится и свойство целостности) или реализация атаки «отказ в обслуживании».

Несмотря на сложности в точном толковании термина «инсайдер», очень немногие специалисты по информационной безопасности пытаются ответить на вопрос о том, что же такое инсайдерская атака. Этот термин касается не только злонамеренных действий сотрудников и других потенциальных инсайдеров, но и более широкого набора нежелательных угроз, которые могут привести к повреждению данных: чтение компьютером дисковых, флэш- и других накопителей сомнительного содержания; запуск вложения к электронному письму, пришедшему от неизвестного отправителя и т.д. По мнению зарубежных специалистов в области компьютерной безопасности Е. Шульца (E. E. Schultz) и Р. Шамвэя (R. Shumway), инсайдерские атаки — это злонамеренное использование компьютерных систем пользователями, уполномоченными на доступ к ним.

Инсайдерские атаки могут быть вызваны рядом причин, как рациональных (возможность извлечь финансовую выгоду, получить желаемую должность, обрести дополнительные полномочия), так и иррациональных, основанных на эмоциях и чувствах, таких как желание отомстить, самоутвердиться, недовольство рабочей обстановкой, глубокие эмоциональные переживания и т.д. В настоящее время психологи активно занимаются изучением эмоционально неустойчивых сотрудников организаций. Это недавно зародившееся направление исследований сможет пролить свет на причины возникновения инсайдерских атак.

Условно инсайдерские атаки можно классифицировать по степени преднамеренности действий их инициаторов.

Злонамеренные инсайдеры могут перехватить частную переписку, украсть или уничтожить данные, использовать информацию в обход политики безопасности, заблокировать доступ к ресурсам автоматизированной системы для остальных пользователей. В зависимости от мотивов враждебных действий, злонамеренных инсайдеров относят к одной из четырех категорий: обиженные, нелояльные, внедренные и подрабатывающие.

Обиженные нарушители стремятся нанести вред компании, исходя из личных побуждений. В большинстве случаев их мотивирует чувство обиды за то, что их недостаточно высоко ценят (недостаточный размер заработной платы, неподобающее место в корпоративной иерархии, отсутствие корпоративных статусных атрибутов и т.д.).

К нелояльным инсайдерам относят сотрудников, решивших сменить место работы. Чаще всего они создают копии данных, с которыми они работали. Например, увольняющиеся сотрудники коммерческих отделов уносят с собой копию клиентской базы, сотрудники отдела финансов — копию финансовой базы.

Как правило, обиженные и нелояльные инсайдеры не представляют серьезной угрозы для организации, так как они сами определяют объект хищения и место его сбыта, из которых первое не всегда оказывается технически доступным, а последнее не всегда удается найти. Однако если до хищения информации обиженный или нелояльный

сотрудник выйдет на потенциального покупателя конкретной информации (конкурент, пресса, криминальные структуры), то благополучие организации окажется под большим сомнением.

Внедренные и подрабатывающие инсайдеры — это сотрудники, цель которых определяет заказчик похищения информации. И в том, и в другом случае они стараются совершить свои действия как можно более незаметно для окружающих. Внедренные инсайдеры — это сотрудники, устроившиеся на работу в целях промышленного шпионажа. К подрабатывающим инсайдерам относят более широкий круг сотрудников — это и люди, решившие подзаработать на ремонт квартиры или покупку машины, и те, кого шантажом и вымогательством вынуждают идти на какие-то действия. Для достижения поставленной цели подрабатывающие инсайдеры могут сымитировать производственную необходимость, пойти на взлом или подкупить других сотрудников.

Незлонамеренные инсайдеры — это пользователи, которые совершают ошибки, компрометирующие информационную безопасность. В эту группу также входят пользователи, мотивированные желанием самостоятельно исследовать и «усовершенствовать» компьютерную сеть предприятия и допускающие при этом грубые нарушения правил безопасности. Не имея ни капли злого умысла, они могут открыть путь для атак извне, случайно уничтожить данные, нарушить целостность и доступность информационных ресурсов и тем самым подвергнуть опасности всю организацию.

К другой категории незлонамеренных инсайдеров относятся сотрудники, действующие под руководством злоумышленника, использующего методы социальной инженерии. Многие хакеры признаются, что при осуществлении атаки на систему им редко приходится прибегать к техническим методам, так как зачастую люди просто дают им всю необходимую информацию. Следует понимать, что социальная инженерия — это самый простой путь свести трудновыполнимую внешнюю атаку к менее сложной внутренней. Поэтому в интересах организации проинформировать сотрудников об известных приемах социальных инженеров.

Прогнозирование инсайдерских атак

В идеале, организации должны уметь предсказывать инсайдерские атаки и пресекать их подобно тому, как тайные правительственные организации могут обнаружить и пресечь действия потенциальных шпионов в собственных рядах путём создания их профилей. Существуют различные модели прогноза инсайдерского поведения, многие из которых имеют практическую основу. Эти модели описывают множество видов потенциально опасных мотивов, поступков, симптомов, многие из которых бывают едва заметны и поэтому могут остаться не выявленными. Например:

1. Черты характера.
- Лица, совершающие инсайдерские атаки, зачастую обладают определёнными чертами характера, а именно: интроверсией и депрессивностью, неспособностью справиться со стрессом или конфликтом, злопамятностью, мстительностью и т.д.
2. Вербальное поведение.
- Лица, намеревающиеся осуществить злонамеренные действия, часто намекают окружающим о своих намерениях.
3. Модели использования системы.
- Существуют стандартные модели использования систем, описывающие порядок действий внутренних злоумышленников во время сеанса работы (например, несанкционированные попытки пользователя получить доступ к учетной записи другого человека). Анализ на основе таких моделей сможет выявить злонамеренность даже в тех действиях пользователя, которые на первый взгляд не будут вызывать никаких подозрений с точки зрения политики безопасности.
4. Отрицательные условия работы.
- Негативные или враждебные условия работы также часто связаны с ростом числа инсайдерских атак.
5. Подготовительные действия (например, разведывательные мероприятия) могут свидетельствовать о надвигающейся инсайдерской атаке.
6. Значимые ошибки.
- Начиная атаку, инсайдеры обычно допускают ошибки, и некоторые из них могут выдать вредительские намерения до того, как инсайдер осуществит злонамеренное действие. Вредитель может, к примеру, ошибиться одним-двумя знаками в деструктивной команде, такой как, например, rm –rf / *.* в Unix-системе. Распознавание значимых ошибок в реальном времени может позволить администраторам безопасности быстро предотвратить надвигающиеся атаки с помощью принятия защитных мер (к примеру, завершения удалённого сеанса злоумышленника).
7. Намеренно оставленные метки.
- Инсайдеры могут намеренно оставлять метки (например, враждебные комментарии в одном или нескольких конфигурационных файлах), свидетельствующие о реализованной инсайдерской атаке. Скорейшее обнаружение таких меток позволит предотвратить дальнейшие действия злоумышленника.

В дополнение к сказанному, мотивы инсайдерских атак могут быть в целом охарактеризованы как враждебность, жажда мести и/или наживы. В совместном исследовании, проведенном Координационным центром CERT и Секретной службой США, 57 процентов осуществивших ИТ-саботаж инсайдеров были раздражены, 84 процента руководствовались местью, а 92 процента всех инсайдерских атак произошли вскоре после рабочего инцидента. Злоумышленники по большей части занимали технические должности (86%) и имели привилегированный доступ к системе (90%).

Учитывая растущий объём знаний, предоставляемых исследователями инсайдерских атак, составление точных персональных характеристик для прогнозирования и мониторинга деструктивного поведения не является сверхзадачей. Тем не менее существуют обстоятельства, препятствующие подобному профилированию, и связаны они с законодательством и неприкосновенностью частной жизни. Однако из каждого правила есть исключение, которым в данном случае являются тайные правительственные организации.

Обнаружение инсайдерских атак

Обнаружить инсайдерскую атаку до того, как произойдут очевидные потери, разрушения и/или сбои, бывает очень сложно. Инсайдерские атаки осуществляются людьми, которые, как правило, уполномочены на доступ к вычислительным ресурсам организации и поэтому их поведение в процессе атаки кажется нормальным (безопасным для системы). Но это впечатление может быть обманчиво. Даже за стандартным обращением к файлу может скрываться очень серьезная инсайдерская атака, однако средства обнаружения вторжений (СОВ) и средства предотвращения вторжений (СПВ) обычно не сигнализируют о событиях подобного рода, так как в большинстве случаев тревога являются ложной.

Стоит отметить, что за последние годы способность СОВ идентифицировать внешние атаки стала намного лучше, чего не скажешь об обнаружении внутренних атак. И дело не только в том, что многие действия пользователей при внутренней атаке кажутся безвредными для системы. В большинстве случаев внешние атаки протекают с генерацией сетевого трафика, ко-

торый проходит не только через роутеры и свитчи (служащие в качестве промежуточных звеньев сети), но и через устройства (включая СОВ и межсетевые экраны), расположенные во внешних шлюзах, не говоря уже о многочисленных устройствах внутренней сети организации. Такое количество контрольных точек, несомненно, увеличивает вероятность обнаружения вредоносного трафика. Что касается внутренних атак, то многие из них протекают вообще без генерации сетевого трафика.

К счастью, СОВ — не единственное средство обнаружения инсайдерских атак. Существует множество других разработок, существенно различающихся между собой по принципам функционирования и решаемым задачам. Рассмотрим каждое в отдельности.

Средства «tripwire»

Средства «tripwire» («tripwire» в переводе с английского — верёвка или проволока, натянутая где-либо незаметно, чтобы проходящий человек споткнулся о неё) доступны и как программы с открытым исходным текстом, и как коммерческие продукты. Средства «tripwire» отслеживают изменения в файлах, директориях и регистрационных журналах. Они идентифицируют попытки внутренних злоумышленников установить руткиты (скрывают следы присутствия злоумышленника или вредоносной программы в системе), backdoor-вирусы (предоставляют удаленному компьютеру неправомочный доступ к рабочей машине пользователя) и другие типы вредоносного программного обеспечения.

Система обнаружения аномалий

Системы обнаружения аномалий идентифицируют отклонения от «обычного» (законного) поведения пользователя, контролируя такие параметры, как дата и время сеанса работы, занятость центрального процессора и памяти, используемые команды, скорость печатания и т.д.

Известен случай, когда система обнаружения аномалий идентифицировала атаку на хост-систему Solaris. Поздно ночью злоумышленник вошел в систему от лица зарегистрированного пользователя и запустил компиляцию программы, написанной на языке С. Эти действия сильно отличались от стандартного поведения пользователя, заключавшегося в просмотре веб-страниц и использовании хоста в качестве сервиса электронной почты, на что система обнаружения аномалий отреагировала сигналом тревоги.

Обнаружение утечки данных

Средства обнаружения утечки данных (Data Extrusion Detection) сообщают о наличии ключевых слов (например, «собственность», «деловая инициатива», «технические исследования») в передаваемых файлах, мгновенных сообщениях, постах и статусах в социальных сетях и так далее. Они способны идентифицировать инсайдерские атаки, цель которых — кража секретной информации. Некоторые средства обнаружения утечек оставляют специальные метки на важных файлах, чтобы сгенерировать сигнал тревоги в случае, если кто-то помимо пользователей, не подлежащих анализу (к примеру, владельцев данных), попытается загрузить данный файл.

Одним из лучших способов обнаружения атаки на секретные данные является использование средств управления событиями (Security Information Event Management, SIEM). Они собирают регистрационные данные системы и анализируют их на предмет взаимосвязи. Данные аудита, полученные от большого многообразия источников — межсетевых экранов, сетевых СОВ, серверов, виртуальных частных сетей и т.д.— сравниваются с образцами (паттернами) и подвергаются идентификации. В отличие от обнаружения внешних атак, идентификация внутренних атак часто зависит от отыскания множества тонких, едва различимых нитей, собрав которые в единое целое, можно установить связь между событиями. Чтобы данное утверждение не было голословным, рассмотрим следующие примеры.

Факт обращения к файлу, хранящемуся на хосте, сам по себе ничем не примечателен. Однако последующее отправление копии файла в виде вложения к электронному письму увеличит подозрительность первого события. Если к тому же получатель письма будет иметь сомнительную связь с данной организацией, степень подозрения возрастет в несколько раз и достигнет критической отметки. Выявление взаимосвязанных цепочек событий (загрузка файла — передача файла по электронной почте — адресат письма не принадлежит организации) не составляет труда для средств управления событиями SIEM, в то время как стандартные системы обнаружения вторжений не рассчитаны на решение задач подобного рода.

Средства SIEM эффективны и при обнаружении других едва заметных признаков инсайдерской атаки, таких как безуспешные попытки входа в систему, распределенные во времени. Попытка войти в систему под одним логином с одного хоста, через полчаса — под другим с другого, и так далее — стандартная политика злонамеренных инсайдеров, старающихся избежать обнаружения. СОВ, как правило, замечают эти попытки войти в систему, но не видят связи между ними, в то время как средства SIEM обнаруживают взаимосвязь данных событий и квалифицируют их как попытку осуществления инсайдерской атаки.

Заключение

В обозримом будущем инсайдерские атаки ещё будут представлять серьёзную угрозу для информационной безопасности организаций. Задачу предсказания и борьбы с ними существенно усложняет многообразие факторов (технических, административных, психологических), обусловливающих злонамеренные действия.

Несомненно, использование передовых программно-технических средств защиты от инсайдерских атак — это серьезное подспорье для обеспечения информационной безопасности организации. Однако не стоит забывать, что ИТ-безопасность складывается из ряда компонентов, которые также нельзя упускать из виду. Это административные (информирование сотрудников о методах социальной инженерии) и психологические меры (тщательный отбор кадров и профилирование сотрудников, анализ психологического состояния сотрудников в течение рабочего сеанса). Только грамотное сочетание этих компонентов позволит достичь успеха в предотвращении инсайдерских атак и борьбе с ними, защитит организации от серьезных потерь.

Список литературы

1. Kenneth Brancik, Insider Computer Fraud: An in-Depth Framework for Detecting and Defending Against Insider IT Attacks, CRC Press, November 2007.
2. S. Kumar, Classification and Detection of Computer Intrusions, Ph. D. Dissertation, Purdue University, Lafayette.
3. T. Tuglular & E. H. Spafford, A framework for characterization of insider computer misuse, Purdue University, 1997.
4. E. E. Schultz & R. Shumway, Incident response: A strategic guide for system and network security breaches.
5. N. Einwechter, Preventing and detecting insider attacks using IDS, on-line document, http://online.securityfocus.com/infocus/1558.
6. E. E. Schultz, «A framework for understanding and predicting insider attacks,» Computers and Security, 21 (6) (2002), стр.526–531.
7. D. M. Capelli, Management and education of the risk of insider threat (MERIT) Mitigating the risk of sabotage to employer's information, systems or networks, 2007, www.cert.org/archive/pdf/merit.pdf.
8. A. Chuvakin, «Log Analysis vs. Insider Attacks», ISSA Journal, November 2007, стр.36–39.