С. Ж. Симаворян (Сочи, СГУТиКД)**. Применение методов Data Mining для обнаружения инсайдеров.**

Инсайдеры — это компьютерные «несуны», ворующие информацию в своей фирме и продающие ее конкурентам. Инсайдерская атака — это утечка персональной и конфиденциальной информации. Среди прочих киберпреступлений инсайдерские атаки имеют самый высокий уровень латентности (сокрытия) и самый низкий показатель раскрываемости.

В настоящее время, для анализа посещений баз данных (БД) фирмы, широко применяются статистические показатели оценки посещаемости сайтов, показывающие количество обращений к БД. Недостатками применения статистических показателей являются то, что они не во всех случаях адекватно отражают степень информированности сотрудника фирмы о БД в целом, т. к. не учитывают структуры связей между страницами БД, и тем более не показывают какие данные БД пользуются наибольшей популярностью. Более качественную информацию об осведомленности сотрудников фирмы о БД и ее содержании дает применение методов Data Mining, в частности применение алгоритма поиска регулярных эпизодов. Целями анализа поведения сотрудников предприятия по использованию БД являются: оптимизация структуры БД; оптимизация разрешений на выполнение операций READ, WRITE, определение статистики посещений каждой страницы БД, которая показывает тематическую направленность интересов сотрудников предприятия; а также выявление попыток несанкционированного доступа к элементам БД, если такое есть на предприятии. Обычно информация о посещениях БД извлекается из лог-файла СУБД, т. е. из того сервера где расположена сама БД, но для решения названных целей она не достаточна.

Для реализации указанной целей предлагается: 1) сформировать информационный кадастр БД [1] на основе данных хранящихся в БД; 2) реализовать подход, основанный на применении методов Data Mining (поиска регулярных эпизодов) для анализа данных информационного кадастра. При этом под информационным кадастром понимается полная и хорошо структурированная совокупность данных, отражающая структуру БД на различных уровнях (тематическом, структурном, файловом, разрешительном и т.д.) [2]. Информационный кадастр удобно представить в виде упорядоченной совокупности так называемых объектно-характеристических таблиц (ОХТ), каждая из которых представляет собой таблицу, в строках которой находятся наименования тех реалий сайта (предметов, событий, явлений или обобщенно — объектов), а по столбцам — наименования тех характеристик учитываемых объектов, значения которых необходимы для информационного анализа (обеспечения) функционирования сайта; сами значения характеристик располагаются в соответствующих клетках ОХТ.

Для заполнения информацией таблиц ОХТ предлагается использовать специально разработанные программы, выполняющие последовательное сканирование всех страниц БД. При сопоставлении информации из указанных таблиц посредством стандартных SQL запросов в сочетании с применением методов Data Mining (поиском регулярных эпизодов), становится возможным более детальный и глубокий анализ поведения сотрудников и других пользователей, который позволяет своевременно выявлять и пресекать инсайдерство на предприятии. Для эффективной защиты от инсайдеров в первую очередь необходимо обеспечить контроль над всеми коммуникационными каналами — от обычного офисного принтера до обычной флэшки и фотокамеры мобильника.

Методы защиты от инсайдеров: 1) аппаратная аутентификация сотрудников (например, с помощью USB-ключа или смарт-карты); 2) аудит всех действий всех пользователей (включая администраторов) в сети; 3) использование мощных программно-аппаратных средств защиты конфиденциальной информации от инсайдеров; 4) обучение сотрудников, отвечающих за информационную безопасность; 6) повышение

личной ответственности сотрудников; 7) постоянная работа с персоналом имеющим доступ к конфиденциальной информации — инструктаж, обучение, проверка знаний правил и обязанностей по соблюдению информационной безопасности и т. д.; 9) соответствие уровня зарплаты уровню конфиденциальности информации; 10) шифрование конфиденциальных данных.

Но самое главное, конечно, человеческий фактор: хотя человек — самое слабое звено в системе безопасности, но и самое важное. Борьба с инсайдерами не должна превращаться в тотальную слежку всех за всеми. В компании должен быть здоровый моральный климат, с соблюдением морально-этическим норм.

СПИСОК ЛИТЕРАТУРЫ

1. *Чубукова И. А.* Data mining. ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2008, 384с.
2. *Герасименко В. А.* Основы информационной грамоты. Энергоатомиздат, 1996, 320 с.