Математические структуры и моделирование
2014. № 4(32). С. 236–239

УДК 658.511:004.056

СИСТЕМА ВЫЯВЛЕНИЯ ИНСАЙДЕРОВ

В.С. Веденеев
ведущий спец-т по информационной безопасности (ОАО «ЧЦЗ»),
e-mail: ingafen@gmail.com
И.В. Бычков
д.ф.-м.н., проф., e-mail: bychkov@csu.ru

Челябинский государственный университет

Аннотация. В статье рассмотрен опыт создания системы выявления инсайдеров на основе самоорганизующихся сетей Кохонена.

Ключевые слова: самоорганизующиеся сети Кохонена, инсайдер.

1. Введение (описание проблемы)

Задача поиска инсайдеров в информационных системах предприятий является одной из основных, стоящих перед службой информационной безопасности. Инсайдер обладает большим набором полномочий для выполнения своих должностных обязанностей, что даёт ему возможность воспользоваться своими полномочиями для нанесения ущерба предприятию.

Ущерб может быть экономическим, репутационным, в некоторых случаях может привести к нарушению работы предприятия (например, в случае вывода из строя серверного или коммутационного оборудования). Выделяют следующие виды инсайдерских атак [1]:

1. Мошенничество
2. Саботаж
3. Кража интеллектуальной собственности.

Выявление инсайдерской атаки, за исключением крайних случаев, представляет собой трудновыполнимую задачу. Необходимо из общего потока информации и событий выделить те, которые являются вредоносными.

Такие события могут соответствовать заранее установленным правилам или паттернам — например: копирование конфиденциальной информации на неучтённые носители, попытки входа под чужим аккаунтом, подбор паролей и т.п. Однако в большинстве случаев инсайдерские атаки представляют собой действия, которые вполне могут показаться легитимными. Отличить в таком случае вредоносные действия от рабочих задач можно лишь в рамках контекста, который можно назвать «нормальной работой». То есть той работы, которую «обычно» делает данный субъект. Построение такого контекста является трудновыполнимой задачей. В большинстве случаев, контекст строится, исходя из эмпирических знаний и опыта.

2. Варианты решений

Одним из первых математических решений была система IDES, разработанная Дороти Деннинг (Dorothy E.Denning) [2]. Система устанавливала профиль активности работы пользователя на ПК. Её система была рассчитана на терминального пользователя, однако, может быть и расширена для обычных пользователей системы.

Разработано большое количество средств защиты информации, направленных на выявление инсайдерских атак. В первую очередь — это DLP-системы (data leakage protection — предотвращение утечек информации). DLP-системы контролируют потоки информации, циркулирующие через ПК, с целью выявления передачи конфиденциальных данных. Функционал DLP-систем достаточно широк. Однако в большинстве случаев DLP-системы могут лишь зафиксировать факт утечки информации. Несмотря на то что DLP-системы обладают функцией блокировки передачи информации, этой опцией пользуются крайне редко. Это связано с тем, что блокировка может существенно снизить скорость информационного обмена предприятия с окружающим миром, т.к. принятие решения специалистом по безопасности о передаче данных после их блокировки занимает некоторое время.

Кроме того, некоторые DLP-системы включают в себя системы мониторинга работы пользователя на ПК — какие программы он запускал, сколько времени провёл в системе и т.д.

Также к системам выявления инсайдеров можно добавить системы Honey-pot, Honey-net и им подобные [3,4]. Honey-pot представляют собой системы, которые представляются сетевыми сервисами, однако, напрямую не используются и открыто не публикуются. Основная их цель — привлечь внимание нарушителя, который проводит разведку внутри сети. Любое обращение к Honey-pot можно рассматривать в качестве инсайдерской атаки. Honey-net представляет собой несколько honey-pot, объединённых в одну сеть.

Таким образом, существует некоторое количество инструментов, которые позволяют выявлять инсайдерские атаки по заранее определённым паттернам или правилам.

Помимо выявления инсайдерских атак крайне перспективным направлением является предсказание инсайдерских атак, а именно — выявление личностей, склонных к инсайдерской деятельности.

3. Предлагаемое решение

В своей работе мы рассмотрели возможность применения самоорганизующихся сетей Кохонена для выявления инсайдеров в корпоративных информационных системах. Выбор сетей Кохонена в качестве математического аппарата системы был сделан по следующим причинам:

1. Сети Кохонена относятся к сетям с «обучением без учителя», что позволяет автоматически строить упомянутый выше контекст.

2. Сети Кохонена способны проводить кластеризацию информации, тем самым проводить автоматическое разбиение элементов на группы.

3. На основе кластеризации удобно производить поиск аномалий.

Основная идея состоит в следующем: на основе мониторинга действий пользователя выявлять аномальную деятельность, деятельность, которая может соответствовать инсайдерской деятельности. На основе этих данных строить портрет/образ пользователя.

Сети Кохонена выступают в двух ролях: во-первых, служат инструментом для выявления аномальной деятельности, во-вторых, служат инструментом для обобщения данных о пользователе.

В программе использована библиотека CUDAfy.NET для работы с графическими адаптерами, произведёнными компанией NVidia, NoSQL база данных Redis. Redis был выбран в связи с высокой скоростью работы. Основным его ограничением является тот факт, что при работе база данных выгружается в ОЗУ. В связи с этим в будущем при использовании больших массивов данных Redis будет использоваться в качестве кэширующей базы данных, а в качестве основной будет использоваться одна из «традиционных» реляционных баз данных.

Графический интерфейс программы выполнен с использованием технологии WPF (Windows Presentation Foundation) и паттерна MVVM (Model-View-ViewModel). Использование паттерна MVVM дало возможность быстро перестраивать графический интерфейс при изменении логики программы. Это дало возможность изучать сети Кохонена в интерактивном режиме, а также подбирать оптимальный способ обнаружения аномальных действий пользователя.

На текущий момент реализован поиск аномалий среди веб-активности пользователя (посещение интернет-сайтов), авторизационных данных (входах/выходах из системы), запускаемых процессов и программ, активность работы с файловой системой. Данные вводятся в программу вручную.

В связи с тем, что получение реальных инсайдерских данных — это трудновыполнимая задача, то проверка работоспособности системы производится на уровне интеграционных тестов.

Ближайшие планируемые работы — расширение областей, среди которых ведётся поиск аномалий, а также — построение слоя для обобщения данных и непосредственно — построения портрета пользователя.

4. Заключение

Использование сетей Кохонена для поиска инсайдеров в корпоративных информационных системах является перспективным направлением, требующим проработки при создании реальных систем. Сети Кохонена имеют большой потенциал распараллеливания, что позволяет добиться высокой производительности всей системы.

Литература

1. Cappelli D.M., Trzeciak R.F., Floodeen R. The Key to Successful Monitoring for Detection of Insider Attacks.
2. Denning D. An Intrusion-Detection Model // IEEE Transaction on Software Eng. 1987. Feb. C. 222–232.
3. Even L.R. Intrusion Detection FAQ: What is a Honeypot? 2010. July. URL: `http://www.sans.org/security-resources/idfaq/honeypot3.php`
4. Spitzner L. Honeypots: Catching The Insider Threat // Computer-Security Application Conference. Proceesings, 19th Annual. 2003.

INSIDER DETECTION SYSTEM

Victor S. Vedeneev
Postgraduate Student, e-mail: ingafen@gmail.com
Igor V. Bychkov
Professor, Doctor of Physical and Mathematical Sciences, e-mail: bychkov@csu.ru

Chelyabinsk State University

Abstract. Insider detection system based on Kohonen self-organizing neural network is described in this work.

Keywords: Kohonen self-organizing neural network, insider.