УДК 004.01

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ И ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ

А.М. Кадан, А.П. Сальников, П.С. Французов

В условиях роста количества ставших достоянием общественности инцидентов утечек информации, рассматривается задача создания учебного стенда программного продукта «InfoWatch Traffic Monitor 4.1» для демонстрации и изучения возможностей систем защиты информации от внутренних угроз. Использование учебного стенда позволило вести современное практико-ориентированное обучение студентов таких высокотехнологичных специальностей как, в частности, 1-98 01 01-01 Компьютерная безопасность и 1-26 03 01 Управление информационными ресурсами. Подобный учебный стенд создан в вузе Республики Беларусь впервые.

В современном информационном обществе эффективное применение информационных технологий является общепризнанным показателем конкурентоспособности компании. Электронная коммерция, продажа информации, оказание консультаций в онлайн-режиме и многие другие подобные виды услуг становятся для ряда предприятий в условиях цифровой экономики основными видами деятельности.

Безусловно, что корпоративная информация всегда является ценным ресурсом, вне зависимости от формы представления: электронной или «бумажной», однако нельзя не обращать внимания на тот факт, что при переносе информации в среду корпоративных информационных систем повышаются риски ее неправомерного использования, что может привести к ощутимым финансовым потерям.

Всё больше корпоративных систем, приложений и данных становятся доступными из Глобальной сети, вследствие чего компании сталкиваются с возрастающим числом различных угроз: несанкционированный доступ, вирусы, утечки информации и т.д. Все это повышает важность задач связанных с обеспечением защиты информации.

Немного аналитики

Аналитический Центр компании InfoWatch на протяжении многих лет занимается отслеживанием публикаций об утечках информации в открытых источниках и анализом факторов, влияющих на формирование глобальной картины утечек данных. В отчете об исследовании утечек конфиденциальной информации в I полугодии 2015 года особое внимание уделяется изучению последствий, которыми оборачиваются утечки данных [1].

Сообщения об утечках не сходят с полос ведущих СМИ, что связано как с масштабом явления (компрометация данных миллионов пользователей), так и с громкими именами компаний, пострадавших от утечек, ставших достоянием общественности. В числе таких организаций только за I полугодие 2015 года: Anthem, Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Equifax, FIA, Google, HBO, HSBC, HTC, JP Morgan Chase, Kia Motors, Lenovo, Lufthansa,

Microsoft, Morgan Stanley, NVIDIA, PayPal, PwC, Samsung, Starbucks, Tele2, Toyota, Twitter, Uber, United Airlines, Yahoo [1, с. 4].

Данные отчета подтверждают, что количество случаев утечки конфиденциальной информации на 10% превышают количество утечек, зарегистрированных за аналогичный период 2014 года. Внешние атаки стали причиной 32% утечек данных, причем доля таких утечек выросла на 9 % по сравнению с показателем I полугодия 2014 года. 90% утечек связаны с компрометацией персональных данных. За I полугодие 2015 года были похищены более 262 млн записей, в том числе платежная информация. Зафиксированы 8 «мега-утечек», в результате каждой из которых «утекли» персональные данные более 10 млн человек. В 58% случаев виновными в утечке информации оказались сотрудники компаний. В 1% случаев – высшие руководители организаций (топ-менеджмент, главы отделов и департаментов) [1, с.3].

Важность защиты от внутренних угроз информационной безопасности

Как свидетельствуют статистические данные, за I полугодие 2015 года зарегистрирована 471 (65%) утечка информации, причиной которой стал внутренний нарушитель. В 233 (32%) случаях утечка информации произошла из-за внешнего воздействия. Для некоторых случаев (2,6%) установить вектор воздействия (направление атаки) оказалось невозможно [1, с. 7].

Бесспорно, что из года в год одним из самых важных каналов утечки информации являются сотрудников компании. От потерь конфиденциальной информации, связанной с коммерческими и производственными секретами, личными данными сотрудников, компании несут убытки и, согласно мировой статистике, косвенный ущерб не уступает прямым убыткам. В результате снижается лояльность клиентов, наблюдается их отток, понижается стоимость брендов, страдают имидж и репутация компании.

Необходимость защиты от внутренних угроз, связанных, в первую очередь, с некомпетентностью и нелояльностью персонала, была очевидна на всех этапах развития информационного общества. Чтобы предупредить потерю информации и попытаться облегчить контроль над огромными потоками данных, экспертами в области информационной безопасности были созданы специализированные продукты, известные как DLP-системы (DLP – Data Loss Prevention). Хотя, исторически, внешние угрозы считались более критичными, в последние годы на внутренние угрозы стали обращать пристальное внимание и популярность DLP-систем значительно возросла.

DLP-системы создают защищенный периметр вокруг организации, анализируя входящий и исходящий трафик, документы, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемые на принтерах и т.

Механизмы детектирования конфиденциальной информации

Для того чтобы препятствовать утечкам конфиденциальной информации, DLP-система имеет специальные механизмы определения конфиденциальности документа.

На сегодняшний день выделяют пять типов анализа:

1) Поиск по словарям (по точному совпадению слов, с учетом морфологии).
2) Регулярные выражения - система синтаксического разбора текстовых фрагментов по формализованному шаблону, основанная на системе записи образцов для поиска. Например, номер кредитной карты, номер телефона, адрес электронной почты, номер паспорта, лицензионные ключи и т.д.
3) Сравнение по типам файлов - политиками безопасности может быть запрещена отправка вовне некоторых типов файлов. При этом если пользователь изменит расширение файла, то система все равно должна «опознать» тип файла и предпринять необходимые действия. В большинстве решений используется технология компании Autonomy [2].
4) Технологии цифровых отпечатков - достаточно сложные технологии, при которых производятся определенные математические преобразования исходного файла (алгоритмы преобразований производителями не раскрываются). Процесс преобразования строится по схеме: исходный файл - математическая модель файла - цифровой отпечаток. Это позволяет существенно сократить объем обрабатываемой информации (объем цифрового отпечатка не более 0,01 от объема файла). Цифровые отпечатки размещаются в базе данных (Oracle, MS SQL) и могут быть продублированы в оперативной памяти устройства, осуществляющего анализ информации. Отпечатки затем используются для сравнения и анализа передаваемой информации. При этом отпечатки передаваемого и «модельного» файлов могут совпадать не обязательно на 100%, процент совпадения может задаваться (или запрограммирован в ПО производителем).
5) Статистический («поведенческий») анализ информации по пользователям - если пользователь имеет доступ к конфиденциальной информации и в то же время он посещает определенные сайты (web-storage, web-mail, хакерские и т. д.), то он попадает в «группу риска» и к нему возможно применение дополнительных ограничивающих политик безопасности.

Указанные технологии устойчивы к редактированию файлов и применимы для защиты практически любых типов файлов: текстовых, графических, аудио, видео. Количество «ложных срабатываний» не превышает 1% (все другие технологии дают 20-30% ложных срабатываний).

Современные DLP-системы обычно сочетают несколько таких технологий, применяемых в зависимости от совокупности проявлений угроз в конкретной ситуации.

Задача подготовки специалистов в области защиты от утечек данных

Развитие рынка DLP-систем делает актуальной задачу подготовки специалистов в области защиты информации и компьютерной безопасности, которые бы достаточно компетентно владели технологиями конфигурирования, использования и расширения возможностей DLP-систем, методами анализа

инцидентов информационной безопасности и предотвращения таких инцидентов.

С этой точки зрения представляется актуальной задача интеграции в учебный процесс профильных специальностей современных технологий защиты информации от внутренних угроз либо в форме отдельных специальных дисциплин, либо в форме практико-ориентированных средств или учебных стендов для поддержки лабораторного практикума в рамках существующих учебных программ.

Необходимость и актуальность проведения работ обусловлена также повышенным интересом к проблемам защиты данных организаций и активным ростом на этом фоне востребованности DLP-систем, необходимостью изучения систем подобного класса студентами профильной специальности, формирования в обществе адекватного отношения к задачам информационной безопасности и защиты компьютерных данных.

Учебный стенд программного продукта «InfoWatch Traffic Monitor 4.1»

В работе представлен опыт создания учебного стенда программного продукта «InfoWatch Traffic Monitor 4.1» для демонстрации и изучения функционала и возможностей систем защиты информации от внутренних угроз, использование которого позволит вести современное практико-ориентированное обучение студентов таких высокотехнологичных специальностей как, в частности, 1-98 01 01-01 Компьютерная безопасность и 1-26 03 01 Управление информационными ресурсами. Подобный учебный стенд был создан на кафедре системного программирования и компьютерной безопасности в 2015 году, впервые в вузе Республики Беларусь.

Стенд позволил демонстрировать технологии решения целого класса задач из области защиты информации: предотвращения утечек и контроля перемещения конфиденциальной информации за пределы организации, предотвращения утечек персональных данных и клиентских баз, защиты интеллектуальной собственности, применения целевых политик контроля персонала входящего в т.н. «группы риска», расследования инцидентов информационной безопасности и пр.

Учебный стенд программного продукта «InfoWatch Traffic Monitor» создан в рамках договора о международном сотрудничестве ГрГУ им. Я.Купалы и компании АО «ИнфоВотч» (Российская Федерация) и представляет собой DLP-систему систему, адаптированную к использованию в условиях факультета вуза.

Возможности учебного стенда

Назначение учебного стенда – использование в учебном процессе всех ИТ-специальностей факультета математики и информатики, в первую очередь специальностей 1-98 01 01 «Компьютерная безопасность» и 1-26 03 01 «Управление информационными ресурсами», для проведения курсового и дипломного проектирования, в научно-исследовательской работе преподавателей кафедры системного программирования и компьютерной безопасности, для подготовки новых спецкурсов.

Программное обеспечение стенда допускает контроль таких каналов утечки, как передача данных по протоколам SMTP, HTTP, HTTPS, копирование файлов на сменные носители, печать документов на локальных и сетевых принтерах, службы обмена мгновенными сообщениями Skype, Jabber, ICQ, хранение документов на рабочих станциях и сетевых папках.

В настоящее время учебный стенд позволяет контролировать перемещение данных на персональных компьютерах, включенных в домен факультета математики и информатики, выполнена настройка его конфигурации и формирование учебной базы данных инцидентов.

Особенности конфигурирования учебного стенда

Учитывая потенциальные возможности стенда, должное внимание было уделено конфигурированию подсистемы сбора и анализа данных и ограничению доступа к базе инцидентов. Выполнена, в соответствии с особенностям работы вуза, настройка подсистемы, выполняющей анализ текста перехваченных объектов с помощью методов лингвистического анализа (определение тематики текста на основании найденных терминов), детектирования текстовых объектов (поиск в тексте таких объектов, как номера телефонов, паспортов, кредитных карт и пр.), детектирования цифровых отпечатков (поиск в фрагментов, относящихся к конфиденциальным данным).

Также, поскольку работа в домене факультета предполагает авторизацию пользователей через LDAP-сервер, в учебных целях для снижения потенциального объема инцидентов, из категории детектируемых пользователей были исключены сотрудники факультета, лаборанты кафедр, учебно-вспомогательный персонал. Это позволило избежать многих конфликтных ситуаций, хотя негативно сказалось на темпах формирования базы инцидентов системы, поскольку перехватывался только трафик, проходящий через стационарную сеть факультета, а студенты, в силу использования беспроводных вычислительных устройств, практически перестали использовать оборудование компьютерных классов.

Заключение

За время эксплуатации, с апреля 2015 года, учебный стенд использовался в ходе изучения отдельных тем дисциплин «Теоретические основы информационной безопасности» специальности «Компьютерная безопасность» и «Управление информационной безопасность» специальности «Управление информационными ресурсами». Демонстрация его работы и выполнение студентами позволили отметить глубокое осознание последними проблем защиты организации от внутренних угроз и методов их решения, что не могло быть достигнуто в такой мере при чисто теоретическом обучении.

Также к учебному стенду были подключены рабочие станции четырех компьютерных классов факультета математики и информатики. Это позволило получить обширную статистику использования средств вычислительной техники на факультете и скорректировать стратегию их использования.

Работы по конфигурированию и развертыванию учебного стенда выполняются в рамках реализации договора о международном сотрудничестве между ГрГУ им.Я.Купалы и АО «ИнфоВотч» (Российская Федерация).

Список литературы

1. Аналитический центр InfoWatch. Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года / Сайт компании InfoWatch, 2003-2016. - Режим доступа: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015_half_year.pdf. - Дата доступа: 27.03.2016.
2. Autonomy has joined HP / Hewlett-Packard Development Company. L.P., 2016. - Режим доступа: http://autonomy.com/. - Дата доступа: 27.03.2016.
3. Кадан, А. М. Использование DLP-системы в подготовке специалистов по защите информации / А.М. Кадан, М.К. Рудь, П.С. Французов, В.И. Цидик // Технические средства защиты информации: сборник тезисов докладов XIII Белорусско-российской науч.-техн. конф., Минск, 4-5 июня 2015 г. - Мн.: БГУИР, 2015. – С.93-94.

Кадан Александр Михайлович, заведующий кафедрой системного программирования и компьютерной безопасности УО «Гродненский государственный университет имени Янки Купалы», кандидат технических наук, доцент, kadan@mf.grsu.by

Сальников Андрей Петрович, АО «ИнфоВотч» (Российская Федерация), представитель в Республике Беларусь, Andrey.Salnikov@infowatch.com

Французов Павел Сергеевич, стажер компании АО «ИнфоВотч» (Российская Федерация), магистрант УО «Гродненский государственный университет им. Янки Купалы», francuzov_ps_10@mf.grsu.by