УДК 004.4:004.056.5:004.62

РАЗРАБОТКА СИСТЕМЫ, ПРЕДНАЗНАЧЕННОЙ ДЛЯ АНАЛИЗА АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ

Тамбовцев Г.А., Маркова А.А., Косых А.В.

Воронежский институт высоких технологий, Воронеж, e-mail: app@vivt.ru

Работа посвящена исследованию вопросов, связанных с информационной безопасностью. Нет возможностей для того, чтобы полным образом устранить риск внутренних атак, но можно максимально сократить вероятность их возникновения, предприняв необходимый комплекс мер. Проведено рассмотрение некоторых из них: использование политик с минимальными привилегиями пользователя, использование продуктов фильтрации почтового контента, шифрование конфиденциальной информации. Разрабатываемая программа предназначена для сбора аналитической информации о действиях пользователей на компьютере и сохранения её в файл для последующего его просмотра и анализа. Для реализации программного решения описанной выше задачи удаленного администрирования были выбраны: в качестве языка программирования C# и C++, в качестве среды программирования – Microsoft Visual Studio 2012.Программа представлена файлом с настройкой пути к лог – файлу, лог – файлом, двумя исполняемыми файлами.

Ключевые слова: защита информации, программа, передача данных

THE DEVELOPMENT OF A SYSTEM FOR ANALYZING USER ACTIVITY

Tambovtcev G.A., Markova A.A., Kosykh A.V.

Voronezh Institute of High Technologies, Voronezh, e-mail: app@vivt.ru

The paper is devoted to the study of issues related to information security. There are no opportunities to fully eliminate the risk of internal attacks, but you can minimize the likelihood of their occurrence by taking the necessary measures. Reviewed some of them: use policies with minimal user privileges, use of the products of filtering mail content, encryption of confidential information. Develop programs designed to collect analytical data about user activity on the computer and save it in a file for subsequent viewing and analysis. For the implementation of the software solutions described above tasks remote administration was selected as the programming language of C# and C++ as the programming environment – Microsoft Visual Studio 2012.The program presents a file by setting the path to your log file, log file, two binary files.

Keywords: information protection, program, data transfer

Внутренние атаки чаще всего совершаются людьми, которые имеют доступ к сети и системам. Это могут быть любые люди, злоупотребляющие своими привилегиями, такие как недовольные сотрудники, или материально ответственные люди, или временные работники, или соискатели, устраивающиеся на работу с целью взлома.

В связи с этим стоит ожидать различные ситуации [1–3], такие как преднамеренное заражение компьютеров, с целью нарушить работу, внедрение шпионских программ для получения информации о деятельности сотрудников, для кражи паролей или копирования конфиденциальной информации для дальнейшего использования.

Стратегии построения защиты большинства организаций направлены преимущественно на внешние вторжения. Объясняется это тем, что психологически человеку неприятно думать о том, что предать может кто-то «свой». Основа такой защиты заключалась в межсетевом экране, который стоит между пользователями, сервером и внешним миром. Но часто такой метод бывает ошибочным.

Предприятия защищаются в основном при помощи различных решений безопасности, таких как брендмауэр, системы обнаружения вторжений или унифицированного управления угрозами. Они занимаются фильтрованием сетевого траффика в поисках возможного нежелательного или вредоносного содержимого. К сожалению для таких методов внутренний трафик находится вне досягаемости.

В случае использования IDS перед администраторами сети появляется проблема. Ведь если необходимо защитить сеть изнутри целиком это потребует достаточно больших информационных мощностей и вычислительных ресурсов. К тому же при тотальном контроле повышается нагрузка на сети, что в конечном итоге потребует её перепланировку. Издержки на приобретение компонентов IDS и перепланировку сети могут повлечь сомнения в целесообразности такого подхода. Кроме того даже при максимальных затратах такие системы не обеспечивают защиту от неизвестных типов атак.

Конечно же, невозможно полностью устранить риск внутренних атак, но можно максимально сократить вероятность их возникновения, предприняв необходимый комплекс мер. Рассмотрим некоторые из них.

Использование политик с минимальными привилегиями пользователя, которых хватает только для решения поставленных задач. Этим обеспечивается недоступность данных всем пользователям. Такие данные должны предоставляться только тем пользователям, которым они нужны для работы, а не всем отделам.

Использование продуктов фильтрации почтового контента, например, для блокировки сообщений, содержащих определенные слова. Это необходимо для того, чтобы сотрудник не мог отправить конфиденциальные данные за пределы предприятия.

Необходимо использовать контроль USB устройств для предотвращения выноса информации, отключать USB устройства на компьютерах тех сотрудников, которым они не требуются. Так же с помощью специальных утилит можно вести журнал активности использования USB устройств.

При аудите доступа к файлам сотрудник не должен получать доступ к файлам, которые не нужны ему для работы.

Шифрование конфиденциальной информации усложнит доступ, как во внутренней, так и во внешней сети предприятия.

Это лишь некоторые методы, которые стоит предпринять для защиты своей сети от внутренних угроз.

В связи с тем, что на предприятии установлены компьютеры не высокой производительности, требования к системе обнаружения должны быть низкими. Она должна состоять из программы кейлоггера, который должен отслеживать нажатия клавиш в приложениях и записывать это в лог-файл, который должен располагаться в недоступном месте для пользователя. Лог-файл должен сканироваться системным администратором на предмет выявления угроз, ключевых слов и нажатий клавиш с определенной периодичностью, устанавливаемой самим администратором или контролирующей службой. Должна использоваться программа контроля USB устройств, которая должна вести журнал об интенсивности использования накопителей. Программный продукт должен работать в скрытом режиме и составлять и сохранять отчеты в указанном месте.

В свете требований [4–6], предъявляемых к процессу соблюдения политик ИБ, были рассмотрены возможности, предоставляемые рабочими станциями сети предприятия, указывающие на целесообразность разработки системы слежения за пользователями.

Разрабатываемая программа предназначена для сбора аналитической информации [7–9] о действиях пользователей на компьютере и сохранения её в файл для последующего его просмотра и анализа.

Сформулируем основные требования, предъявляемые к разрабатываемой системе мониторинга активности пользователей.

Во-первых, программный продукт должен отслеживать нажатия клавиш пользователем и отображать, в каком активном окне они были совершены. Это обусловлено необходимостью слежения за действиями пользователей, для выявления нарушения политик информационной безопасности а так же трудовой дисциплины.

Во-вторых, программа должна отслеживать и распознавать подключаемые USB устройства, а так же отслеживать создание, изменение и удаление файлов и папок находящихся на них. Это поможет отследить вынос конфиденциальной информации с предприятия.

В-третьих, программа должна запускаться и работать в скрытом от пользователя режиме, для предотвращения попыток обхода возможностей утилиты. Так же для упрощённого доступа к информации лог – файлы должны называться в соответствии с текущей датой и меняться при наступлении следующей.

В-четвертых, программа должна нормально функционировать в ОС Windows XP/7, быть устойчивой к сбоям, неправильным действиям пользователя, корректно обрабатывать возможные аварийные завершения (отключение питания).

Для реализации программного решения описанной выше задачи удаленного администрирования были выбраны: в качестве языка программирования – C# и C++, в качестве среды программирования – Microsoft Visual Studio 2012. Выбор обуславливается тем, что C# относится к семье языков с C-подобным синтаксисом, из них его синтаксис наиболее близок к C++ и Java. Язык имеет статическую типизацию, поддерживает полиморфизм, перегрузку операторов (в том числе операторов явного и неявного приведения типа), делегаты, атрибуты, события, свойства, обобщённые типы и методы, итераторы, анонимные функции с поддержкой замыканий, LINQ, исключения, комментарии в формате XML.

Программа представлена файлом с настройкой пути к лог – файлу, лог – файлом, двумя исполняемыми файлами.

В программе предусмотрено начало работы при старте системы. Так как программа не имеет интерфейса, при запуске она

никак не оповещает пользователя о активности. Единственное, что может заметить пытливый взгляд пользователя это подозрительное имя процесса, который отображается в диспетчере задач.

Для указания места создания лог – файлов используется файл *. bat в котором в текстовом виде латинскими буквами пишется путь.

При открытии лог-файла можно увидеть сообщение о начале мониторинга, также видно сообщение о нажатии клавиш или их комбинаций и название активного окна в момент нажатия клавиш.

При подключении USB устройства создается сообщение о начале наблюдения или об ошибке, в случае его невозможности и сообщения о создании, изменении или удалении файлов.

При включении компьютера с установленным USB устройством сообщение о начале наблюдения не создается, но отслеживание активности исправно производится.

Перед всеми событиями указывается время, в которое они произошли.

Так же в работе представлена программа, которая сканирует лог файлы по требованию. В процессе выполнения продукт действует по определенным алгоритмам [10] и помечает курсивом подозрительные сообщения. Примеры сообщений, которые должны считаться подозрительными указывает ответственный сотрудник. Все найденные и помеченные сообщения переносятся в отдельный файл, что должно облегчить мониторинг подозрительной активности пользователя.

Программа имеет интерфейс, в котором указывается расположение основного лог – файла и файла предупреждений. Так же в программе присутствует библиотека подозрительных сочетаний клавиш, которые должны отслеживаться.

Выводы по работе. В процессе выполнения данной работы были рассмотрены различные системы анализа активности пользователей и программного обеспечения. Подробно рассмотрены системы отслеживания действий пользователей, такие как кейлоггеры и USB мониторы. Были изучены существующие материалы по данной теме, произведено ознакомление с алгоритмической и методологической базой. На основе произведенного анализа принципов мониторинга был разработан программный продукт на языке C#, выполняющий задачи отслеживания нажатий клавиш и их комбинаций, активных окон во время нажатий, а также распознавание и слежение за USB устройствами.

Список литературы

1. Львович И.Я. Факторы угрозы экономической безопасности государства / И.Я. Львович, А.А. Воронов, Ю.П. Преображенский // Информация и безопасность. – 2006. – Т. 9. № 1. – С. 36–39.

2. Львович И.Я. Применение методологического анализа в исследовании безопасности / И.Я. Львович, А.А. Воронов // Информация и безопасность. – 2011. – Т. 14; № 3. – С. 469–470.

3. Воронов А.А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А.А. Воронов, И.Я. Львович, Ю.П. Преображенский, В.А. Воронов // Информация и безопасность. – 2006. – Т. 9; № 2. – С. 8–11.

4. Пеньков П.В. Экспертные методы улучшения систем управления / П.В. Пеньков // Вестник Воронежского института высоких технологий. – 2012. – № 9. – С. 108–110.

5. Черников С.Ю. Использование системного анализа при управлении организациями / С.Ю. Черников, Р.В. Корольков // Моделирование, оптимизация и информационные технологии. – 2014. – № 2 (5). – С. 16.

6. Преображенский Ю.П. Разработка методов формализации задач на основе семантической модели предметной области / Ю.П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 075–077.

7. Зяблов Е.Л. Разработка лингвистических средств интеллектуальной поддержки на основе имитационно-семантического моделирования / Е.Л. Зяблов, Ю.П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 024–026.

8. Фомина Ю.А. Принципы индексации информации в поисковых системах / Ю.А. Фомина, Ю.П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98–100.

9. Зяблов Е.Л. Построение объектно-семантической модели системы управления / Е.Л. Зяблов, Ю.П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 029–030.

10. Лисицкий Д.С. Построение имитационной модели социально-экономической системы / Д.С. Лисицкий, Ю.П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 135–136.