УДК 681.3

ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

© 2018 Ю. П. Преображенский

Воронежский институт высоких технологий (г. Воронеж, Россия)

В данной работе рассмотрен комплекс мер по обеспечению безопасности корпоративной сети. Указаны актуальные угрозы безопасности. Даны предложения по программному продукту, позволяющему улучшить характеристики безопасности системы.

Ключевые слова: информационная безопасность, корпоративная сеть, защита информации.

Для того, чтобы обеспечить безопасность корпоративной сети, принимается комплекс мер:

- сетевое оборудование размещено в контролируемой зоне;
- сеть сегментирована, определены правила размещения ресурсов в сегментах;
- правила доступа в интернет установлены и контролируются;
- выход в публичные сети контролируют межсетевые экраны, настроенные в соответствии с политикой ИБ;
- сетевые сервисы сконфигурированы в соответствии с политикой ИБ, изменения в настройках контролируются;
- имеется резервное оборудование и резервные копии для восстановления работы ключевых сервисов;
- журналы Log-файлов и результатов аудита защищены от уничтожения на период установленного срока хранения;
- системы, обеспечивающие работу критически важных серверов и активного сетевого оборудования, спроектированы как высоконадежные сервисы;
- антивирусное ПО установлено на всех рабочих станциях и серверах внешнего доступа и регулярно обновляется;
- ИТ персонал проводит аудит сетевой активности с использованием средств мониторинга.

Для обеспечения режима информационной безопасности удаленного доступа принимаются такие меры:

- конфигурирование программно-технических средств, осуществляющих удаленный доступ к ресурсам корпоративной сети;
- применяются стандартные правила обеспечения информационной безопасности, включая аспекты:
  - аутентификация и учетные записи;
  - установление и разрыв соединений;
  - права доступа к внутренним ресурсам;
  - контроль IP удаленных клиентов;
  - криптографическая защита сеансов с использованием встроенных в Windows Server средств;
  - регистрация событий в журналах и аудит.

Одними из актуальных угроз безопасности информационной среды на предприятиях, использующих корпоративную сеть, являются следующие:

- получение несанкционированного доступа к информации за счет воздействия на программное обеспечение;
- получение несанкционированного доступа к информации за счет физического проникновения в помещения, в которых расположены носители информации, средства обработки информации, средства коммуникации;
- получение несанкционированного доступа к информации путем доступа к каналу связи и (или) коммутационному оборудованию;
- блокирование доступа к информации из-за перегрузки (недоступности) сетевых ресурсов;
- получение несанкционированного доступа к информации внешним нарушителем путем хищения носителя информации и средств обработки информации за пределами контролируемой зоны;
- разглашение, уничтожение, блокирование или изменение информации вследствие неумышленного запуска/установки ПО, содержащего вредоносный код;

Преображенский Юрий Петрович – Воронежский институт высоких технологий, к. т. н., доцент, профессор ВИВТ, oimk@vivt.ru.

- разглашение, уничтожение, блокирование или изменение информации вследствие неумышленного внедрения вредоносного программного обеспечения при использовании сменных носителей информации / ноутбука;
- неумышленное разглашение информации за счет передачи ее за пределы организации с использованием каналов связи Интернет;
- разглашение/блокирование доступа к информации вследствие умышленного хищения носителя информации, средств обработки информации (ноутбука);
- хищение информации за счет преднамеренного копирования информации на нештатные носители информации;

умышленное изменение или уничтожение (стирание) информации;

Нестандартное поведение сотрудника может быть вызвано следующими факторами:

- редкие плановые отчеты, обычно не проводящиеся сотрудником;
- отсутствие сотрудника на рабочем месте и использование этого рабочего места другим сотрудником или посторонним человеком;
- занятие сотрудником делами, не связанными с рабочими процессами и обычно не выполняемыми;
- вирусная активность, вызванная новым вирусом и не отслеживаемая антивирусом;
- действия сотрудника, вызванные случайными факторами;
- злонамеренные действия сотрудника, связанные с подготовкой к планируемому увольнению;
- злонамеренная кража коммерческой информации в крупных объемах, не проводившаяся ранее;

У разных сотрудников разные обязанности, разное, типичное для конкретного сотрудника, выполнение своих функциональных задач. Также различные сотрудники используют рабочие инструменты в нерабочих целях.

Несмотря на то, что основная бизнес-информация компании хранится на серверах баз данных (MySQL), пользователи рабочих мест работают за персональными компьютерами, имеющими локальные хранилища информации. Также сотрудники ведут служебную переписку, создают служебные документы, сохраняют мультимедийный файлы с использованием своих рабочих станций.

В связи с различиями, как задач, так и поведения людей, использовать универсальный продукт для контроля каждого рабочего места сотрудника, не представляется возможным. Однако, используя методы построения самообучающихся систем, возможно создать программный продукт, подстраивающийся под каждого конкретного сотрудника, под конкретные, выполняемые им задачи.

Для защиты информации от случайных или злонамеренных действий сотрудников, а также рабочих мест сотрудников в случае их компрометации злоумышленником, необходимо создать и внедрить программное обеспечение (далее – Продукт), подстраивающееся под штатные, регламентируемые действия сотрудников, которые выполняются чаще всего в процессе операционной деятельности данных сотрудников, и реагирующее на нестандартное поведение сотрудников.

Продукт должен состоять из клиентской, серверной и административной частей, а также базы данных, связанной с Продуктом.

Клиентская часть Продукта должна запускаться на компьютерах сотрудников в качестве службы и заниматься сбором данных о текущей деятельности сотрудника путём отслеживания сеансов обращения к жесткому диску. Клиентская часть Продукта должна отправлять собранные данные на серверную часть Продукта.

При отслеживании обращений к жесткому диску должны учитываться следующие данные:

- имя пользователя системы, производящего обращение к жесткому диску;
- имя процесса, с помощью которого инициируется обращение к жесткому диску;
- системное время, в которое произошло обращение к жесткому диску;
- тип операции с жестким диском (чтение, запись);
- имя файла, созданного на жестком диске;
- объем данных, записанных на жесткий диск/считанный с диска;
- расположение файла на жестком диске.

Серверная часть Продукта должна принимать данные от клиентской части. Каждая клиентская часть должна обрабатываться независимо от других клиентских частей. Далее будут описаны принципы обработки данных касательно одного клиента. Эти же методы

применяются ко всем остальным клиентским частям независимо друг от друга.

Присланные данные собираются в реляционную базу данных. В базе данных должна быть создана структура, позволяющая быстро обращаться и находить любое значение из присланных данных.

После периода сырого сбора данных серверная часть должна обобщить присланные данные, чтобы выделить основные патерны поведения пользователей. Обобщение данных предполагается проводить алгоритмами сравнения, применительно к каждому типу присланных данных, применяя заданный коэффициент соответствия (далее Коэффициент).

Далее серверная часть работает в режиме анализа присылаемых клиентской частью данных. В случае совпадения присланных данных с находящимися в базе в пределах отклонения, задаваемых Коэффициентом, серверная часть принимает эти данные, как регулярные и не реагирует на событие.

В случае, если присланные данные выходят за рамки отклонения, задаваемого Коэффициентом, серверная часть должна среагировать на событие и оповещать ответственных лиц путём отправки сообщений на Email или SMS. Также данное событие должно журналироваться и создавать интерфейс взаимодействия в административной части.

Административная часть должна отслеживать рабочие станции, которые подключены к Продукту и на которых запущена клиентская часть. Рабочие станции могут иметь несколько статусов:

- сбор данных;
- регулярная работа;
- предупреждение о инциденте, 1 степень (в случае, если коэффициент отклонения от регулярной деятельности рабочей станции достаточно мал);
- предупреждение о инциденте, 2 степень (в случае, если зафиксировано малое количество отклонений от регулярной деятельности рабочей станции);
- предупреждение о инциденте, 3 степень (в всех остальных случаях).

Администратор Продукта должен иметь возможность просмотреть событие, вызвавшее инцидент и принять по нему решение. Решения должны быть следующих типов:

- регулярное событие, не реагировать по нему в дальнейшем;
- просмотрено, не предпринимать никаких действий;
- атипичный инцидент, начать запись действий рабочей станции.

Продукт должен соответствовать следующим требованиям:

- стабильная работа при одновременной работе до 500 клиентских рабочих станций;
- время реагирования на событие не более 10 секунд;
- возможность задания времени сбора информации;
- возможность задания Коэффициента;
- клиентская часть должна работать под управлением ОС Microsoft Windows версий 7-10;
- серверная часть должна работать под управлением любой серверной ОС;
- административная часть должна работать в браузере Microsoft Internet Explorer, Google Chrome (и подобные), Mozilla Firefox и быть кросс-платформенной.

ЛИТЕРАТУРА

1. 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.

2.Гуськова Л. Б. О построении автоматизированного рабочего места менеджера / Л. Б. Гуськова // Успехи современного естествознания. – 2012. – № 6. – С. 106.

3.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.

4. 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.

5.Максимов И. Б. Классификация автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 127-129.

6. Максимов И. Б. Принципы формирования автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 130-135.

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

8. Преображенский Ю. П. Оценка эффективности применения системы интеллектуальной поддержки принятия решений / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 116-119.

9. Самойлова У. А. О некоторых характеристиках управления предприятием / У. А. Самойлова // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 176-179.

10. 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.

ABOUT SECURITY IN THE CORPORATE NETWORK

© 2018 Yu. P. Preobrazhensky

Voronezh Institute of High Technologies (Voronezh, Russia)

In this paper we consider a set of measures to ensure the security of the corporate network. Actual security threats are indicated. Proposals are given for a software product that allows to improve the security characteristics of the system.

Key words: information security, corporate network, information security.