УДК 004.056

РЕКОМЕНДАЦИИ ПО ПРОТИВОДЕЙСТВИЮ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ НА ПРЕДПРИЯТИИ

Богиня И.Г.[1], Мешков В.И.[2]
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: big94@ua.fm[1], local@i.ua[2]

В данной статье рассматриваются основные методы противодействия распространённым уязвимостям действующих ИС, позволяющих инсайдерам путем несанкционированного доступа к аппаратным и программным средствам системы нарушать свойства обрабатываемой информации.

Ключевые слова – методы и средства защиты информации; противодействие инсайдерской деятельности.

ВСТУПЛЕНИЕ

Согласно отчета украинской компании «СБК» (компании-аудитора ИБ, а также поставщика систем защиты от утечек информации), каждая пятая компания в Украине несла убытки от кибератак, более 70% компаний имеют крайне неэффективную антивирусную защиту, а большинство сотрудников, ответственных за работу с электронными счетами, слабо представляют способы защиты от несанкционированного доступа к этим счетам.

К сожалению, одним из уязвимых мест любой системы всегда остается человек. Работодатель не может быть уверен в полной лояльности и порядочности своих сотрудников. В процессе проектирования систем защиты часто не учитываются кажущиеся незначимыми особенности построения, которые, тем не менее, могут сыграть решающую роль в вопросах защиты информации.

ОСНОВНАЯ ЧАСТЬ

Приведем некоторые практические рекомендации по противодействию инсайдерской деятельности на предприятии:

1. Действенным, но, тем не менее, не всегда используемым решением в области защиты информации, является контроль доступа в помещение, где находится какой-либо узел ИС. Получение программного доступа там, где это не предусмотрено – задача, решение которой под силу лишь квалифицированным пользователям. С другой стороны, кража устройства физически доступна почти каждому.

2. При создании домена чаще всего автоматически создаются две учетные записи – гостя и администратора с соответствующими именами. Для осложнения подбора входных данных к учетной записи администратора для получения обширных полномочий в системе, следует переименовать запись администратора.

3. Стоит отключить возможность использования личных внешних носителей информации сотрудников компании, т.к. по умолчанию во многих ОС включена функция запуска с носителя файла autorun.inf при подключении внешнего устройства к системе. Данный файл мог быть модифицирован злоумышленником: к примеру, в файл могли быть внедрены скрипты, повышающие полномочия пользователя в системе до администратора.

4. В случае, когда запрещено использование внешних носителей информации, утечка может произойти через каналы электронной почты. Необходимо ограничить список лиц, которые могут писать внешним пользователям.

5. Используя прокси-сервер, необходимо запретить использование облачных хранилищ, а также запретить использование распространенных протоколов передачи файлов таких, как FTP для недопущения загрузки на вышеописанные сетевые ресурсы информации компании.

6. Эффективным решением, направленным на противодействие нарушению конфиденциальности и доступности информации и ресурсов, является использование систем обнаружения/предотвращения утечек информации (системы DLD/DLP) [3]. Существует два кардинально разных подхода по использованию вышеописанных систем:

- недопущение утечек любой информации (использование DLP-систем);
- допущение утечки определенной информации с последующим анализом цепочки получателей данной информации.

7. При выборе DLD/DLP-системы стоит учесть возможность шифрования файловых систем внешних носителей информации самой системой обнаружения/предотвращения утечек. Данная функция позволяет использовать только зарегистрированные устройства, выданные сотрудникам самой организацией. Это обеспечивает невозможность использования данных внешних устройств где-либо вне рассматриваемой ИС.

8. В случае, когда в ходе анализа угроз выявлена вероятная кража носителей информации, возможно использование Rights Management Services - технологии защиты документов на базе службы каталогов Microsoft Active Directory путем шифрования с применением ограничений доступа и лицензий доступа, позволяющей сохранять ограничения даже после загрузки и открытия файла пользователем.Технология требует поддержки со стороны клиентского ПО, применяемого для работы с документами; такую поддержку имеют Microsoft Office начиная с версий 2007 Enterprise, Professional Plus и Ultimate. AD RMS возможно использовать параллельно с другими технологиями такими, как

смарт-карты. Так же необходима поддержка со стороны клиентской ОС; в MS Windows 7/Vista/8/8.1 и Windows Server 2008/2012 включён клиент AD RMS [2].

9. В случае, когда пользователь системы имеет доступ к сетевому расположению с зашифрованными файлами (т.е. кража носителя информации не даст результата по причине отсутствия ключа расшифрования), то во время работы с файлом с помощью прикладного ПО сам файл хранится на клиентской системе как временный файл в незашифрованном виде. Из-за ошибок работы ОС и модулей памяти после выключения системы и даже после закрытия сеанса работы с приложением-редактором рассматриваемого файла, у пользователя есть возможность извлечь полезную информацию из случайно сохраненного временного файла. В качестве контрмеры, можно перенести все каталоги, где хранятся временные файлы, на сервер, к которому у пользователя не будет доступа, или переместить временные каталоги на RAM-диск, область в ОЗУ, определяемой ОС в качестве жесткого диска, содержимое которого будет уничтожено после выключения системы.

10. Исключить проблему НСД инсайдера к информации, хранящейся на клиентской машине, возможно путем виртуализации клиентских ОС. В данном случае, пользователь должен будет подключаться к удаленному рабочему столу, из-за чего на клиентской машине будет обрабатываться лишь принимаемое потоковое видео, а не сама информация, с которой работает сотрудник. Однако, использование стандартного протокола RDP не является наилучшим решением. По умолчанию, протокол RDP предоставляет общий буфер обмена для клиентской и виртуальной ОС, что является каналом утечки информации. Также, присутствует возможность подключения внешних дисков, с которых также можно скопировать данные. Решением данной проблемы является использование терминального сервера, контролирующего использование виртуальных рабочих столов, или использование таких протоколов, как PC-over-IP, предоставляющих только лишь потоковое видео и ничего более, перекрывая каналы утечки [1].

ЗАКЛЮЧЕНИЕ

Уровень эффективности вышеописанных методик напрямую зависит от того, насколько своевременно, квалифицированно, полно и комплексно они реализованы. Необходимо отметить, что при решении задачи противодействия инсайдерской деятельности ключевыми факторами успешности являются как уровень профессионализма специалистов, внедряющих данные методики, так и степень понимания руководством компании важности и необходимости принимаемых мер.

ССЫЛКИ

1. Мєшков В.І., Маслов Д.М. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МАНІПУЛЮВАННЯ СВІДОМІСТЮ КЛІЄНТІВ БАНКУ ЯК ЗАГРОЗА ОТРИМАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ. – 2014.
2. Мешков В.И., Дашко Д.А., СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. – 2013.
3. Михеев М. О. Администрирование VMware vSpere 5. М.: Буки Веди, 2012. - 505 с.
4. Р. Моримото, М. Ноэл, Г. Ярдени, О. Драуби, Э. Аббат, К. Амарис. Microsoft Windows Server 2012. Полное руководство. М.: Вильямс, 2013. – 1456 с.
5. Богиня Г.А. Тезисы доклада «Выявление инсайдеров: Практический опыт. Тонкости проведения служебных расследований с помощью аналитического модуля КИБ SI», г. Сочи, закрытая конференция по информационной безопасности.