КОД БЕЗОПАСНОСТИ

115127, Россия, Москва а/я 66
+7 (495) 982-30-20
info@securitycode.ru
www.securitycode.ru

Комментарий разработчика ООО «Код безопасности» к статье «Сравнение эффективности средств защиты информации от несанкционированного доступа» и одноименной презентации на форуме Positive Hack Days 2017

Приводятся комментарии компании – разработчика СЗИ Secret Net 7 – ООО «Код безопасности» к статье «Сравнение эффективности средств защиты информации от несанкционированного доступа» (расположена по ссылке) авторства Алфёрова Романа Игоревича и Горохова Андрея Александровича (ООО «Стандарт безопасности», г. Ярославль).

О модели нарушителя

Авторами статьи при анализе эффективности СЗИ Secret Net 7 сделано неверное предположение о потенциальном нарушителе (см. раздел 1.2 статьи).

В эксплуатационной документации на продукт СЗИ Secret Net (см. раздел 9.5 Формуляра на СЗИ Secret Net 7) приведено указание по эксплуатации: обеспечить запрещение предоставления штатным пользователям защищенного компьютера привилегий администратора средства. Если учетная запись пользователя входит в группу локальных администраторов, то данный пользователь является администратором СЗИ Secret Net 7.

Таким образом, нарушитель третьего уровня (согласно Руководящему документу «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации») должен быть исключен из рассмотрения.

Результаты тестирования

Для следующих проверок, выполнявшихся авторами статьи в ходе сравнения эффективности средств защиты информации, использовались административные привилегии, что противоречит требованиям, приведенным в эксплуатационной документации на СЗИ Secret Net 7:

- прямое чтение с жесткого диска (разделы 3.1.2 и 3.2.1 статьи);
- устойчивость к атакам типа НСД, осуществляемым из-под системных учетных записей (раздел 3.2.2 статьи);
- наличие противодействия атакам типа НСД в режиме ядра (раздел 3.2.4 статьи);
- противодействие управлению настройками СЗИ от НСД из-под системных учетных записей (раздел 3.3.1 статьи);
- противодействие деактивации модулей СЗИ от НСД (раздел 3.3.2 статьи);
- стойкость защиты конфигурационных файлов СЗИ от НСД (раздел 3.3.3 статьи);
- функционирование СЗИ от НСД в безопасном режиме (раздел 3.3.4 статьи);
- изоляция модулей (раздел 3.4 статьи).

Если СЗИ Secret Net 7 эксплуатируется в соответствии с рекомендациями, приведенными в эксплуатационной документации на продукт, данные угрозы не могут быть реализованы в защищаемой информационной системе.

Рекомендации разработчика

Отдельно остановимся на угрозе получения доступа к теневым копиям защищаемых ресурсов (раздел 3.1.1 статьи) и угрозе утечки защищаемой информации через различные объекты ОС (раздел 3.2.3 статьи).

1. Угроза получения доступа к теневым копиям защищаемых ресурсов использует службу теневого копирования тома (Volume Shadow Copy), которая входит в состав ОС Windows и по умолчанию включена.

   Для работы с теневой копией не требуются полномочия администратора, пользователи могут восстанавливать предыдущие версии файлов из таких снимков в случае, если у них есть на это права NTFS.

   Для получения доступа защищаемым файлам, нарушитель с привилегиями обычного пользователя может воспользоваться функцией просмотра предыдущих версий файла, получив доступ к теневой копии.

Рекомендация разработчика: данную угрозу необходимо нейтрализовать с помощью отключения службы теневого копирования тома системным администратором ОС Windows на защищаемых средствах вычислительной техники.

Соответствующие рекомендации будут внесены в эксплуатационную документацию на продукты.

2. Угроза утечки защищаемой информации через различные объекты ОС использует возможность запуска двух параллельных сеансов работы пользователей с разными уровнями конфиденциальности. С помощью механизмов межпроцессного обмена или сетевого взаимодействия осуществляется обход механизм контроля потоков: информация с более высоким уровнем конфиденциальности может быть передана пользователю, работающему под более низким уровнем конфиденциальности.

Рекомендация разработчика: отметим, что угроза потенциально направлена на механизм полномочного (мандатного) управления доступом, требование к применению которого формулируется по умолчанию для автоматизированных систем, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну.

Данная угроза нейтрализуется с помощью включения механизма замкнутой программной среды в жестком режиме (к запуску разрешено то, что явно указано администратором) с контролем целостности исполняемых файлов. При выполнении данных рекомендаций пользователь не будет иметь возможность запуска программ, не относящихся напрямую к обработке информации ограниченного доступа.

Дополнительно администраторам безопасности необходимо следить, чтобы в информационной системе не использовалось ПО, содержащее скрытые каналы утечки информации. Для исключения утечки информации по сети, необходимо настроить категории конфиденциальности на сетевых адаптерах.

Соответствующие рекомендации будут внесены в эксплуатационную документацию на продукты.