направлений информационной безопасности являются научные исследования учёных СНГ как практические исследования в той же области компании Cisco Systems, Inc.?

Для ответа на вопрос проанализируем результаты работ по защите информации в облаке известного на Украине коллектива исследователей под руководством академика Украины, д т н., профессора В. С. Харченко [3] (Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт»). Среди работ коллектива ввиду ограниченного объёма этой публикации рассмотрим только три статьи – работы [4–7]. В [4–6] рассматриваются только DDoS-атаки на облако. В [7] анализируются только стандарты информационной безопасности для облачных технологий и тенденции их развития.

Коллектив из БГУИР (д. т. н., профессор В. А. Вишняков и его аспирант М. М. Гондаг Саз) в своих работах [8–11], опубликованных в реферируемом журнале, рассматривает только проблемы аутентификации пользователей в облаках. Здесь, правда, неясно, используют ли модели аутентификации в облачных вычислениях для мобильных приложений из статьи [10] алгоритмы аутентификации пользователей в мобильной среде из тезисов [11] (в [11] нет упоминаний об облаках, поэтому может показаться, что данные алгоритмы пригодны везде, а не только в облачных вычислениях).

ВЫВОД: по состоянию на сегодня ни о какой комплексности научных исследований в области безопасности облаков учёных СНГ с точки зрения числа рассматриваемых направлений информационной безопасности по сравнению с практическими направлениями аналогичных исследований учёных дальнего зарубежья не может быть и речи.

Список использованных источников:

1. Отчет. Cisco по информационной безопасности за первое полугодие 2017 г. – Сан-Хосе (Калифорния): Cisco Systems, Inc., июль 2017. – 90 с.

2. Журавлёв, М. С. Краткий обзор украинских работ по защите данных в облаках / М. С. Журавлёв // В наст. сборнике.

3. Профессор Вячеслав Сергеевич Харченко: библиографический указатель к 60-летию со дня рождения / И. В. Олейник, В. С. Гресь, К. М. Нестеренко, В. М. Новичкова. – Харьков, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт». 2012. – 258 с.

4. Меленец, А. В. Защита Cloud-архитектур от DDoS-атак / А. В. Меленец // Радіоелектронні і комп'ютерні системи. – 2013. – № 5 (64). – С. 64–69.

5. Меленец, А. В. Многоверсионная модель защиты облака от DDOS-атаки / А. В. Меленец // Радіоэлектронні і комп`ютерні системи. – 2014. – № 6 (70). – С. 140–144.

6. Melenets, A. The State Corporate Cloud Computing- Based Network for Registration of Potentially Dangerous Objects / A. Melenets // Information & Security: An International Journal. – Sofia, Bulgaria, 2012, – Vol. 28, – N 1 & 2. – P. 52–62.6.

7.Поночовный, Ю. Л. Стандарты информационной безопасности для облачных технологий и тенденции их развития / Ю. Л. Поночовный, А. А. Фурманов, В. С. Харченко // Радіоэлектронні і комп`ютерні системи. – 2015. – № 4 (74). – С. 25–33.

8. Вишняков, В. А. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях / В. А. Вишняков, М. М. Гондаг Саз // Доклады БГУИР. – 2016. – № 3 (97). – С. 111–114.

9. Вишняков, В. А. Концепция и обеспечение безопасности корпоративных информационных систем с использованием облачных вычислений / В. А. Вишняков, М. М. Гондаг Саз, М. Г. Моздурани Шираз // Доклады БГУИР. - 2016. – № 8 (102). – С. 101–102.

10. Вишняков, В. А. Модели аутентификации в облачных вычислениях для мобильных приложений с интеллектуальной поддержкой выбора / В. А. Вишняков, М. М. Гондаг Саз // Доклады БГУИР. – 2017. – № 1 (103). – С. 82–86.

11. Гондаг, С. М. Алгоритмы аутентификации санкционированных пользователей в мобильной среде / С. М. Гондаг, В. А. Вишняков // Технические средства защиты информации: Тезисы докладов XIV Белорусско-российской научно-технической конференции, 25-26 мая 2016 г., Минск. – Минск: БГУИР, 2016. –С. 28–29.

КОМПЛЕКСНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА БАЗЕ ПО NET STUDIO

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Пуйдак В.А.

Пачинин В. И. – зав. кафедрой ИСиТ, канд. техн. наук, доцент

В работе проведен анализ основные методы комплексной защиты персональных данных на основе современных технологий.

Значительную часть работ по защите информации составляют задачи обеспечения безопасности рабочих станций и серверов. Для их решения применяются продукты класса Endpoint Security, которые компенсируют внутренние и внешние угрозы с помощью различных подсистем безопасности (антивирус, СЗИ от НСД, персональный межсетевой экран и др.) [1].

Модель угроз информационной безопасности традиционно включает целый перечень актуальных для рабочих станций и серверов угроз. Угрозы не получалось нейтрализовать одним-двумя средствами защиты информации (далее — СЗИ), поэтому администраторы устанавливали 3-5 различных продуктов, каждый из которых выполнял определенный набор задач: защиту от несанкционированного доступа, вирусов, фильтрацию сетевого трафика, криптографическую защиту информации и т. д.

Такой подход сводит работу администраторов к непрерывной поддержке СЗИ из различных консолей управления и мониторинга. Кроме того, продукты разных вендоров плохо совместимы, что приводит к нарушению функционирования и замедлению защищаемой системы, а в некоторых случаях — и вовсе ко сбою в работе.

Сегодня на рынке появляются комплексные решения, которые объединяют несколько защитных механизмов. Такие СЗИ упрощают администрирование и выбор мер по обеспечению безопасности: у них единая консоль управления, отсутствуют конфликты в работе подсистем безопасности, продукты легко масштабируются и могут применяться в распределенных инфраструктурах. Одним из комплексных средств защиты является продукт Secret Net Studio 8.1, разработанный компанией «Код Безопасности» [2].

СЗИ Secret Net Studio — это комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Продукт объединяет в себе функционал нескольких средств защиты «Кода Безопасности» (СЗИ от НСД Secret Net, межсетевой экран TrustAccess, СЗИ Trusted Boot Loader, СКЗИ «Континент-АП»), а также включает ряд новых защитных механизмов.

В рамках данного продукта решаются следующие задачи:

Защита от внешних угроз:

– защита рабочих станций и серверов от вирусов и вредоносных программ;

– защита от сетевых атак;

– от подделки и перехвата сетевого трафика внутри локальной сети;

- защищенный обмен данными с удаленными рабочими станциями.

Защита от внутренних угроз:

– защита информации от несанкционированного доступа;

– контроль утечек и каналов распространения защищаемой информации;

– защита от действий инсайдеров;

– защита от кражи информации при утере носителей.

Защита входа в систему.

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к компьютеру. К механизму защиты входа относятся следующие средства:

– средства для идентификации и аутентификации пользователей;

– средства блокировки компьютера;

– аппаратные средства защиты от загрузки ОС со съемных носителей (интеграция с ПАК «Соболь»).

Идентификация и аутентификация пользователей.

Идентификация и аутентификация выполняются при каждом входе в систему. В системе Secret Net Studio идентификация пользователей осуществляется по одному из 3-х вариантов: по имени (логин и пароль), по имени или токену, только по токену.

В Secret Net Studio 8.1 поддерживается работа со следующими аппаратными средствами:

– средства идентификации и аутентификации на базе идентификаторов eToken, iKey, Rutoken, JaCarta и ESMART;

– устройство Secret Net Card;

– программно-аппаратный комплекс (ПАК) «Соболь».

Блокировка компьютера.

Средства блокировки компьютера предназначены для предотвращения его несанкционированного использования. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора. Предусмотрены следующие варианты:

– блокировка при неудачных попытках входа в систему;

– временная блокировка компьютера;

– блокировка компьютера при срабатывании защитных подсистем (например, при нарушении функциональной целостности системы Secret Net Studio);

– блокировка компьютера администратором оперативного управления.

Функциональный контроль подсистем.

Функциональный контроль предназначен для обеспечения гарантии того, что к моменту входа пользователя в ОС все ключевые защитные подсистемы загружены и функционируют. В случае успешного завершения функционального контроля этот факт регистрируется в журнале Secret Net Studio. При неуспешном завершении регистрируется событие с указанием причин, вход в систему разрешается только пользователям из локальной группы администраторов компьютера.

Контроль целостности.

Механизм контроля целостности следит за неизменностью контролируемых объектов. Контроль проводится в автоматическом режиме в соответствии с заданным расписанием. Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков (последние только при использовании ПАК «Соболь»).

При обнаружении несоответствия возможны различные варианты реакции на ситуации нарушения целостности. Например, регистрация события в журнале Secret Net Studio и блокировка компьютера.

Вся информация об объектах, методах, расписаниях контроля сосредоточена в модели данных. Она хранится в локальной базе данных системы Secret Net Studio и представляет собой иерархический список объектов с описанием связей между ними.

Дискреционное управление доступом к ресурсам файловой системы.

В состав системы Secret Net Studio 8.1 входит механизм дискреционного управления доступом к ресурсам файловой системы. Этот механизм обеспечивает:

– разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;

– контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;

– запрет доступа к объектам в обход установленных прав доступа;

– независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows. То есть установленные права доступа к файловым объектам в системе Secret Net Studio не влияют на аналогичные права доступа в ОС Windows и наоборот [2].

Персональный межсетевой.

Система Secret Net Studio 8.1 обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации. Подсистема межсетевого экранирования Secret Net Studio реализует следующие основные функции:

– фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;

– фильтрация пакетов служебных протоколов (ICMP, IGMP и т. д.), необходимых для диагностики и управления работой сетевых устройств;

– фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;

– фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);

– фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);

– фильтрация с учетом полей сетевых пакетов;

– фильтрация по дате / времени суток.

Фильтрация сетевого трафика осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n). Авторизация сетевых соединений в Secret Net Studio осуществляется с помощью механизма, основанного на протоколе Kerberos [3].

С его помощью удостоверяются не только субъекты доступа, но и защищаемые объекты, что препятствует реализации угроз несанкционированной подмены (имитации) защищаемой информационной системы с целью осуществления некоторых видов атак. Механизмы аутентификации защищены от прослушивания, попыток подбора и перехвата паролей. События, связанные с работой межсетевого экрана, регистрируются в журнале Secret Net Studio.

Антивирус.

Защитный модуль «Антивирус» в Secret Net Studio 8.1 осуществляет обнаружение и блокировку вредоносного кода по технологии ESET NOD32 [4]. Таким образом, Secret Net Studio позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. При проверке компьютера осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др. Это позволяет обнаружить и заблокировать внешние и внутренние сетевые атаки, направленные на защищаемый компьютер. Благодаря использованию в рамках одного продукта СЗИ от НСД и антивируса время на проверку и открытие файлов составляет на 30% меньше, чем при независимой реализации защитных механизмов.

Шифрование сетевого трафика.

В состав клиентского ПО системы Secret Net Studio 8.1 включен VPN-клиент, предназначенный для организации доступа удаленных пользователей к ресурсам, защищаемым средствами АПКШ «Континент». VPN-клиент «Континент-АП» обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи, по алгоритму ГОСТ 28147-89 [4]. При подключении абонентского пункта к серверу доступа выполняется процедура установки соединения, в ходе которой осуществляется взаимная аутентификация абонентского пункта и сервера доступа. Процедура установки соединения завершается генерацией сеансового ключа, который используется для шифрования трафика между удаленным компьютером и сетью предприятия.

Таким образом, проведенный анализ показывает, что ПО системы Secret Net Studio 8.1 обеспечивает комплексное решение для защиты рабочих станций и серверов, которое обеспечивает защиту информации одновременно на уровне данных, приложений, сети, операционной системы и периферийного оборудования и позволяет осуществлять централизованное управление и мониторинг всех защитных механизмов с возможностью сбора, корреляции, фильтрации и приоритизации событий информационной безопасности. комплексное решение для защиты рабочих станций и серверов, которое обеспечивает защиту информации одновременно на уровне данных, приложений, сети, операционной системы и периферийного оборудования и позволяет осуществлять централизованное управление и мониторинг всех защитных механизмов с возможностью сбора, корреляции, фильтрации и приоритизации событий информационной безопасности.

Список использованных источников.

1. IBA Endpoint Security. [Электронный ресурс].- Режим доступа: http://ibasecurity.com. **-** Дата доступа: 23.02.2018.

2.Методы и средства защиты компьютерной информации. [Электронный ресурс]. – Режим доступа: http://www.volpi.ru/umkd/zki/index.php?man=1&page=37/. - Дата доступа: 23.02.2018.

3.Протокол сетевой аутентификации Kerberos 5. [Электронный ресурс]. – Режим доступа: https://www.ixbt.com/comm/kerberos5.shtml/. Дата доступа: 23.02.2018.

4.Secret Net Studio 8.1 [Электронный ресурс]. – Режим доступа: https://www.securitycode.ru/products/secret-net-studio/. - Дата доступа: 23.02.2018.

5.ESET Technology – The multi-layered approach and its effectiveness. [Электронный ресурс]. – Режим доступа: https://mirror2.esetnod32.ru/technology/ESET-Technology.pdf. - Дата доступа: 23.02.2018.

6.ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-28147-89. - Дата доступа: 23.02.2018.