УТВЕРЖДЕН

643.53262993.00021-01 99- ЛУ

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ «ПАНЦИРЬ+» ДЛЯ ОС MICROSOFT WINDOWS

Технология защиты, реализуемая КСЗИ «Панцирь+»

Подп. и дата	
Инв.№ дубл.	
Взам.инв.№	
Подп. и дата	
Инв.№ подл	

643.53262993.00021-01 99

Санкт-Петербург

2018

Аннотация

В данном документе рассматривается технология защиты, характеризующая назначение Комплексной системы защиты информации «Панцирь+» для ОС Microsoft Windows (далее КСЗИ «Панцирь+»), обозначение 643.53262993.00021–01, Сертификат соответствия ФСТЭК России № 3473 от 17.12.2015. Приведены основные положения реализованной технологии защиты, более детальное их рассмотрение с иллюстрацией соответствующих механизмов представлено в документе «КСЗИ «Панцирь+» – комплексная система защиты информации» по ссылке http://npp-itb.ru/images/docs/alldocs/present.pdf. В документе не приводятся описание действий администратора по работе с сервером безопасности КСЗИ «Панцирь+» или интерфейсом управления настройками клиентской части КСЗИ «Панцирь+», описание действий приводится в документах «Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Руководство администратора. Локальное администрирование» 643.53262993.00021-01 33 01 и «Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Руководство администратора. Удаленное администрирование» 643.53262993.00021-01 33 02.

Оглавление

1. Введение

Вычислительное средство – объект защиты, может быть охарактеризовано иерархией реализуемых в нем ролей:

- роль загрузки системы (BIOS, загрузчик ОС);
- роль «система» (процесс System, системные драйверы, службы, процессы и библиотеки);
- функциональная роль объекта защиты (рабочая станция, терминальный сервер и т.д.);
- роль системного администрирования объекта (системный администратор и средства администрирования);
- роль защиты объекта (администратор безопасности, средства защиты и их администрирования);
- роли интерактивных пользователей (интерактивные пользователи и приложения).

Каждая роль в общем случае характеризуется необходимым и достаточным для нее набором субъектов доступа (пользователь, процесс) и соответствующим для роли необходимым и достаточным набором объектов доступа, ресурсов.

Реализация технологии защиты в общем случае состоит в решении следующих задач:

- локализация режимов работы в рамках соответствующих ролей – по пользователям, процессам, объектам доступа – в рамках каждой роли должны использоваться только необходимые для нее субъекты и объекты доступа, при условии предотвращения несанкционированной возможности изменения их наборов и модификации;
- изоляция режимов работы в рамках различных ролей – для каждой роли должны предоставляться только необходимые и достаточные для ее реализации возможности и способы взаимодействия с другими ролями, при условии предотвращения несанкционированной возможности их изменения и модификации.

2. Ролевая модель доступа к ресурсам информационной системы интерактивных пользователей.

Поскольку в корпоративной информационной системе пользователями обрабатывается не личная, а корпоративная информация, при реализации защиты пользователь должен рассматриваться в качестве потенциального злоумышленника, несущего в себе угрозу инсайдерской атаки.

Под ролью пользователя понимаем его функциональные обязанности по обработке данных в информационной системе (в том числе, открытой и конфиденциальной информации), под сессией, реализующей роль, сформированную для роли технологию обработки данных и необходимые для ее реализации ресурсы. Сессия в общем случае определяет то, каким образом создаются данные в

информационной системе, какими и как приложениями обрабатываются, в том числе, в какой последовательности (управление информационными потоками), каким образом хранятся и передаются между вычислительными и иными ресурсам и т.д.

Задача защиты состоит в формировании под каждую роль сессии, предоставляющей пользователям только необходимые и достаточные условия для обработки данных в рамках соответствующей роли, и в изолировании различных сессий обработки данных. Под различными понимаем сессии, отличающиеся способами и возможностями обработки данных в информационной системе, а также различными уровнями конфиденциальности обрабатываемой информации.

Формируются сессии механизмами разграничения прав доступа к статичным объектам (реализацией разграничительной политики доступа), изолируются механизмами разграничения прав доступа к создаваемым объектам (реализацией разделительной политики доступа).

Особенностью роли является то, что права доступа к ресурсам, в рамках реализующей роль сессии, всех пользователей, включенных в эту роль, совпадают (одна и та же сессия). Это позволяет использовать учетную запись (при необходимости, несколько с одинаковыми правами доступа субъектов к объектам) не для идентификации в информационной системе пользователя, а для идентификации сессии. Сотрудники, реализующие одну роль, при этом будут входить в систему, в том числе, на различных компьютерах под одной и тоже учетной записью. Если один и тот же сотрудник выполняет несколько ролей на одном вычислительном средстве, то доступ к другой сессии реализуется простой сменой пользователя (роли).

В рамках роли, идентифицируемой учетной записью, КСЗИ «Панцирь+» предоставляет возможность разрешать доступ к различным ресурсам отдельными приложениями. Под «профилем» в модели защиты понимается субъект доступа, идентифицируемый двумя сущностями – пользователь, процесс, в ролевой модели – это соответственно роль, процесс. Профилем в разграничительной политике доступа задается то, каким процессом в рамках какой роли, какое право доступа разрешается/запрещается к ресурсу. В общем случае для назначения прав доступа к различным ресурсам для одной роли могут создаваться различные профили. В случае если для различных ролей к какому-либо ресурсу права доступа совпадают, профиль, как субъект доступа к этому ресурсу, может включать в себя несколько учетных записей, идентифицирующих эти роли.

Обработка конфиденциальной информации в информационной системе априори должна регламентироваться для защиты от ее хищений инсайдерами – должны задаваться и реализовываться соответствующей разграничительной политикой доступа способы и правила ее создания, обработки, хранения, в том числе на конкретных файловых устройствах с реализацией организационных мер их защиты, выдачи только на определенные сетевые ресурсы (что

реализуется средством сетевого экранирования из состава КСЗИ «Панцирь+»), печати только на определенных принтерах, при реализации контролируемого к ним физического доступа и т.д. Реализация подобной совокупности технических и организационных мер в значительной мере снизит риски хищения конфиденциальной информации, обеспечивая вероятность реализации подобной угрозы близкой к нулю.

Проблема защиты от хищения инсайдером (санкционированным пользователем) конфиденциальной информации особенно остро становится в том случае, когда на одном вычислительном средстве одному и тому же пользователю предоставляется возможность доступа к обработке как конфиденциальной, так и открытой информации (различные роли). Особенность обработки открытой информации состоит в том, что она не может, да и не должна каким-либо образом регламентироваться.

Решение задачи защиты от хищения (утечки) конфиденциальной информации средствами КСЗИ «Панцирь+» в этом случае состоит в следующем. Для работы с конфиденциальной и открытой информацией создаются различные роли – сессии, запускаемые под создаваемыми для них различными учетными записями. Эти сессии полностью изолируются – по доступу к файловым объектам, к файловым накопителям и к иным устройствам, к сетевым объектам. Задача – предотвратить все возможные способы перемещения данных из сессии обработки конфиденциальной информации в сессию обработки открытой информации, из которой она уже может быть похищена, что может быть реализовано соответствующими разграничительной и разделительной политиками доступа.

Данный подход к защите основан на том, что защищать от хищений следует данные (документы) большого объема (небольшие объемы данных инсайдер просто запомнит). При невозможности их получения из конфиденциальной сессии, для хищения инсайдеру потребуется создание подобных документов вновь в открытой сессии, что существенно ограничивает его возможности.

Принципиальным требованием к реализации ролевой модели доступа является необходимость присвоения прав доступа субъектам, а не задания их в качестве атрибутов объектам, что реализуется встроенными средствами защиты ОС и известными системами защиты информации от несанкционированного доступа (СЗИ НСД).

3. Ролевая модель доступа к ресурсам информационной системы привилегированных пользователей.

Пользователи с правами администраторов, по причине их повышенных полномочий в системе, несут в себе наиболее опасную угрозу инсайдерской атаки, связанную с возможностью

хищения всех обрабатываемых на вычислительном средстве интерактивными пользователями данных. Как следствие, их права должны усекаться, а действия контролироваться администратором безопасности.

Особо опасную угрозу инсайдерской атаки несет в себе системный администратор, в предположении о том, что ему дано право устанавливать в системе исполнимые и командные файлы, т.к. воспользовавшись этим правом, он может создать в системе инструмент (программное средство) для реализации атаки, внедрять вирусы.

Механизм самозащиты КСЗИ «Панцирь+» позволяет реализовать разграничительную и разделительную политики доступа для привилегированных пользователей, включая системных. При этом воздействовать с правами администратора на механизм самозащиты КСЗИ «Панцирь+» (повлиять на работу системы защиты) невозможно. Это позволяет реализовывать в системе иерархию администраторов, в рамках которой администратор безопасности может формировать и реализовывать роли привилегированных пользователей, усекая их права, предоставляемые системой. Например, можно разрешить использование для администрирования только процессы (библиотеки) соответствующих оснасток, можно запретить, или контролировать все действия администратора, связанные с установкой системных и прикладных исполнимых объектов. Реализацией разделительной политики доступа можно запретить доступ ко всем файлам (к данным) создаваемым интерактивными пользователями, при этом инсайдерская атака администратором становится невозможной.

Изолирование работы администратора реализуется в двух направлениях. Во-первых, на уровне загрузки ОС, поскольку он может повлиять на загрузку, загрузив систему без КСЗИ «Панцирь+». С целью решения этой задачи контролируется доступ к переменным BIOS UEFI, в которых хранятся важнейшие параметры загрузки системы, к ним можно осуществить штатный доступ с правами администратора из ОС. Это позволяет реализовать соответствующую атаку на BIOS UEFI, модифицировав соответствующие переменные, либо создав новые, например, изменив порядок загрузки ОС (передать управление загрузчику ОС на другом накопителе) – загрузить систему без КСЗИ «Панцирь+».

КСЗИ «Панцирь+» позволяет разграничивать права доступа субъектов к переменным BIOS UEFI, предотвращая тем самым атаки, направленные на изменение параметров загрузки системы.

Также контролируется доступ к загрузчику ОС – файлу, характеризуемому отсутствием ссылки с буквой, создаваемому ОС автоматически при установке. Этому загрузчику BIOS UEFI передает управление для загрузки ОС. КСЗИ «Панцирь+» позволяет контролировать и разграничивать права доступа к «скрытым» подобным образом объектам, в том числе, к загрузчику ОС.

Во-вторых, права администратора позволяют, используя соответствующие системные вызовы, различными способами повысить их до системных прав, либо иным способом обойти защиту, что должно предотвращаться системой защиты. КСЗИ «Панцирь+» реализуется контроль и разграничение прямого доступа к дискам, к сервисам олицетворения, к инжектированию кода в процесс (системный), к установке глобальных ловушек (перехватчиков или хуков), т.е. все основные системные вызовы, используемые при реализации атак.

Разграничительная и разделительная политики для системных субъектов доступа (системных процессов и служб) обеспечивают невозможность доступа с системными правами к данным, обрабатываемым интерактивными пользователями, и невозможность воздействия на драйверы, реализующие эти политики доступа – драйверы созданы как невыгружаемые, могут взаимодействовать только с системной службой КСЗИ «Панцирь+», активность системной службы контролируется драйвером с принудительным ее перезапуском при несанкционированном останове и т.д. (реализуется механизмом самозащиты КСЗИ «Панцирь+»).

4. Реализация функциональной роли объекта защиты.

Отличием функционирования терминальных серверов является создание отдельных сессий для регистрируемых на сервере пользователей, что осуществляется с использованием сервисов олицетворения системных процессов и их запуска с правами интерактивных пользователей (терминальный сервер – это системный процесс). Для этой функции, в дополнение к сказанному, могут контролироваться и разграничиваться права доступа субъекта – терминальный сервер, идентифицируемого соответствующей запустившей его учетной записью и процессом терминального сервера.

Виртуальные машины Hyper-V в гипервизоре представляют собой процесс «Рабочий процесс виртуальной машины» vmwp.exe, исполнимый файл которого хранится в папке System32, который работает в контексте создаваемого при запуске машины системного пользователя. Этот пользователь нигде не фигурирует в оснастках ОС, т.е. представляет собой такого же «псевдо пользователя», как SYSTEM, LOCAL SERVICE и т.п. Имя этого пользователя в системе выглядит как фиксированный домен «NT VIRTUAL MACHINE» и некий уникальный идентификатор вида GUID. SID такого «пользователя» начинается так «S-1-5-83-…», тогда как SID обычного, интерактивного, пользователя начинается с «S- 1-5-21-…». КСЗИ «Панцирь+» может использоваться, как для защиты внутри гостевой машины, так и устанавливаться на гипервизор. В этом случае каждая виртуальная машина КСЗИ «Панцирь+» идентифицируется как отдельный субъект, а ее образ как отдельный объект доступа.

5. Защита от хакерских атак.

Для реализации атаки хакеру необходим соответствующий инструмент (процесс), позволяющий реализовать запланированные им действия.

В качестве инструмента хакер может воспользоваться вредоносным исполнимым или командным файлом, загрузив и исполнив вредоносный код на защищаемом вычислительном средстве, либо путем наделения легально используемой программы вредоносными свойствами, за счет эксплуатации выявленной и не устраненной в прикладном или системном средстве уязвимости. При этом заражение программы может реализовываться, как с сохранением вредоносного компонента в файл, так и без этого – непосредственно в оперативной памяти.

Для реализации атаки хакеру требуется каким-либо образом доставить вредоносный компонент на атакуемый компьютер. Одним из наиболее опасных способов доставки вредоносного компонента на целевой компьютер корпоративной информационной системы является фишинг. Именно угроза фишинговых атак наиболее опасна для корпоративных приложений, поскольку в данном случае атака может быть хорошо «персонализирована», что позволяет в полной мере использовать для ее реализации методы социальной инженерии, т.к. злоумышленнику достаточно просто получить представление о компании и о конкретных ее сотрудниках в сети Интернет. Другим актуальным способом реализации атаки является хищение учетных данных (идентификатор и пароль) пользователя, в первую очередь, администратора на защищаемом вычислительном средстве, для последующего удаленного доступа к нему с правами данного пользователя.

Применительно к корпоративным информационным системам наиболее актуальны и опасны целевые (точнее, целенаправленные) или таргетированные атаки. Принципиальным отличием целевой атаки, с точки зрения защиты от нее корпоративных систем, является невозможность ее детектирования, как собственно процесса реализации атаки, так и используемых при осуществлении атаки вредоносных компонентов.

Для защиты от хакерских атак в современных информационных системах используются различного рода детекторы (кода, поведения и т.д.), в первую очередь – это адаптированные для использования в корпоративных приложениях антивирусные средства защиты, т.н. системы класса Enterprise Security Suite.

Недостатком подобного решения является то, что детекторы могут эффективно применяться для защиты от массовых атак, характеризуемых тем, что сигнатуры реализованной целевой атаки выявлены и занесены в соответствующие сигнатурные базы (кодов и поведения). Их назначение – не защита от целевых атак, а предотвращение эпидемий. Как следствие, эффективность подобных

средств определяется скоростью формирования сигнатур осуществленных целевых атак, после обнаружения факта их реализации, и доставки обновлений пользователям.

Защита КСЗИ «Панцирь+», в отличие от антивирусных решений, основана на том, что в корпоративных приложениях установка программ должна быть возможна исключительно системным администратором, при условии, что это ему разрешено. Любой исполнимый или командный код, внедренный на вычислительное средство не должны разрешаться к запуску. В этих условиях основную угрозу атаки несет в себе уже не сторонняя программа или командный код, а наделение легально используемых программ вредоносными свойствами, за счет эксплуатации соответствующих уязвимостей. Задача защиты здесь иная собственно в своей постановке от соответствующей задачи защиты личных компьютеров, решаемой антивирусами.

Задача защиты от хакерских атак решается КСЗИ «Панцирь+» в общем виде – реализацией соответствующих разграничительной и разделительной политик доступа, без необходимости детектирования чего-либо.

Защита от внедрения вредоносных программ.

Интерактивным пользователям разрешается исполнение файлов только из папок %SYSTEMROOT% и %ProgramFiles%, которые запрещено модифицировать. Дополнительно может запрещаться создание исполнимых и командных файлов в иных папках. Запрещается доступ к папке КСЗИ «Панцирь+». Дополнительно ставятся на контроль попытки создания файлов с расширением исполнимых, командных, с альтернативными потоками и т.д.

Системным процессам и службам запрещается создание и модификация исполнимых файлов, которые разрешено выполнять по их расширениям. Дополнительно может запрещаться создание командных файлов. Запрещается доступ к папке КСЗИ «Панцирь+».

Защита от исполнения созданных исполнимых и командных файлов. Защита исполнения созданных файлов.

Предотвращается любая возможность любому субъекту (включая системных пользователей) исполнения любого созданного файла. Общность этого решения заключается в том, что не важно то, каким образом файл загружен в систему, то, в каком он виде загружен – зашифрован, заархивирован и т.д., исполнен он быть не сможет, т.к. к создаваемым файлам блокируется команда на исполнение.

Предотвращается любая возможность чтения командными интерпретаторами (соответствующими процессами) создаваемых файлов.

Защита от фишинговых атак.

Фишинговые атаки состоят в наделении вредоносными свойствами браузера, при посещении зараженного сайта по соответствующей ссылке, либо в результате прочтения приложением зараженного почтового вложения.

Защита от атак на браузер реализуется запретом доступа браузера к файлам, созданным иными приложениями. Реализуется разделительной политикой доступа. Если запретить браузеру доступ к файлам, создаваемым почтовым клиентом, то невозможно будет и перейти по ссылке, передаваемой в письме.

Защита состоит в том, что при прочтении процессом файла, полученного по электронной почте, ему запрещается доступ ко всем ранее созданным (размеченным) файлам. Более того, при каждом последующем обращении к подобному сохраненному файлу (поскольку его разметка не изменяется при сохранении), если он пользователем не отнесен к доверенным, приложению будет запрещаться доступ к доверенным файлам, созданным иными приложениями. При этом, в случае прочтения приложением доверенного файла, ему блокируется доступ к недоверенным файлам, а в случае прочтения недоверенного файла, приложением может быть осуществлен доступ к доверенному файлу, но после этого документ уже может быть сохранен (при необходимости) только как недоверенный файл, причем только путем создания нового файла. Для переноса же файла, полученного по электронной почте, в разряд доверенных, пользователю достаточно (если ему это разрешено) воспользоваться возможностью копирования соответствующего файла проводником (разметка файла будет изменена на созданный проводником).

Защита от хищения учетных данных администраторов.

Для получения учетных данных администраторов наиболее распространены атаки на протокол прикладного уровня SMB, реализующего удаленный доступ к разделяемым ресурсам. Эти атаки предполагают получение «хэша» пароля, передаваемого по сети при удаленной аутентификации пользователя. В КСЗИ «Панцирь+» защита от угроз подобных атак реализуется двумя способами.

– Усиление парольной защиты. Состоит в реализации механизма идентификации и аутентификации пользователей. Пароль КСЗИ «Панцирь+» для удаленного входа в систему, отличный от пароля ОС, при удаленной аутентификации пользователей по каналу не передается – передается пароль ОС, но его хищение не позволит использовать скрытые административные общие ресурсы ADMIN$ и IPC$ для удаленного администрирования.

– Локализация рабочего места администратора. Усекается возможность удаленного администрирования всей доменной сети в пределе только с одного компьютера системного администратора.

6. Заключение

Задача защиты от целевых атак – эта самая актуальная сегодня задача, так или иначе решаемая всеми ведущими вендорами в различных странах. Gartner выделяет три основных реализуемых сегодня на практике технологии для обнаружения целевых атак — анализ сетевого трафика, поведенческий анализ на конечных точках и применение «песочницы». Различные, но общие принципы, описанные Gartner, соблюдаются во всех современных продуктах, к которым можно отнести Check Point SandBlast, Fortinet Advanced Threat Protection, Palo Alto Networks WildFire, Proofpoint Targeted Attack Protection, FireEye Threat Intelligence, Kaspersky Anti Targeted Attack Platform, InfoWatch Targeted Attack Detector и т.д., которые, в той или иной мере могут рассматриваться в качестве аналогов КСЗИ «Панцирь+». Т.е. все они основаны на решении различных задач детектирования, что позволяет их рассматривать в качестве средств защиты от массовых атак.

Ключевое отличие КСЗИ "Панцирь+" – решение задачи защиты именно от целевых атак, причем в общем виде, без необходимости детектирования чего-либо, требующего наличия соответствующих сигнатур и сильно влияющего на загрузку вычислительного ресурса, а результат носит вероятностный характер (ошибки первого и второго рода). При этом КСЗИ "Панцирь +" – это комплексная система защиты, позволяющая в комплексе решать задачи защиты от хищений (утечки) информации инсайдерами без какой-либо контентной фильтрации, в том числе, с привилегированными правами, решать задачи идентификации и управления доступом (класс систем IAM), решаемых сертифицированными СЗИ НСД, реализуя в отличие от иных СЗИ НСД ролевую модель доступа, в отличие же от систем класса Privileged User Management (PUM), Privileged Identity Management (PIM), позволяет не только контролировать, но и различными способами усекать возможности системных администраторов.

Большим преимуществом КСЗИ "Панцирь+" является наличие сертификата ФСТЭК России, причем все механизмы защиты из состава КСЗИ сертифицированы и могут легитимно использоваться в соответствующих информационных системах, требующих применения сертифицированных средств защиты информации.