Компания ООО «НПП «ИТБ»

КСЗИ «Панцирь+» – комплексная система защиты класса «Last frontier» от целевых атак

Страница продукта размещена по ссылке: http://npp-itb.ru/products/armourp

Санкт-Петербург, 2017

Общая классификация и источники угроз атак

В общем случае актуальные угрозы атак можно разделить на массовые и таргетированные (или целевые).

Угрозы атак данных классов принципиально различаются, что обусловливает принципиальное отличие требований по реализации защиты от них.

Массовые атаки – это атаки, угрозы которых известны, они уже реализовывались и идентифицированы (выявлены соответствующие сигнатуры кода – используемых вирусов, и аномальные поведения процессов к системе). Такие атаки на практике реализуются хакерами, как правило, невысокой квалификации, как правило, в отношении домашних компьютеров (реализация подобных атак на корпоративные информационные системы особого смысла не имеет, т.к. они легко выявляются на ранних стадиях реализации).

Таргетированные (целевые) атаки, как правило, предполагают использование уязвимостей нулевого дня, о которых еще никому не известно. Эти атаки уже требуют соответствующей квалификации и знаний злоумышленников, они сложны и направлены на объекты, которые могут принести максимальную выгоду. Принципиальным отличием угрозы целевой атаки также является и то, что ее источником может быть как хакер – внешняя угроза, реализующий атаку из внешней сети, так и легальный пользователь, в том числе, и с привилегированными правами - внутренняя угроза.

Вывод. Говоря о реализации эффективной защиты от целевых атак, следует понимать, что задача защиты должна решаться в комплексе, предполагая защиту как от хакерских атак, так и от атак со стороны легальных пользователей корпоративной информационной системы, включая привилегированных пользователей, т.е. как от внешних, так и т внутренних угроз.

Особенности целевой (или таргетированной) атаки

1. Это атаки, направленные в отношении конкретных коммерческих организаций, отраслей производства или государственных ведомств.
2. Объектами атаки являются весьма ограниченные какими-либо рамками или целями конкретные корпоративные информационные системы.
3. Эти атаки не носят массовый характер и готовятся достаточно длительный период.
4. Вредоносное ПО, если оно используется при реализации атаки, специально разрабатывается для конкретной атаки, чтобы штатные средства защиты, достаточно хорошо изученные злоумышленниками, не смогли обнаружить ее реализацию.
5. Для реализации атаки могут использоваться уязвимости нулевого дня.
6. Как правило, целевые атаки используются для кражи информации, которую легко монетизировать, либо для нарушения доступности к критически важной информации.
7. При осуществлении целевой атаки используются те же механизмы взлома, что и при массовых атаках, в частности фишинг. Отличие составляет подготовка атаки с целью предотвращения возможности ее детектирования средствами защиты.
8. После обнаружения и идентификации целевой атаки, уже по итогам ее осуществления, об угрозе этой атаки становится известно, она переходит в категорию «массовых» - может массово использоваться злоумышленниками. При этом, как идентифицированная, угроза этой атаки уже может детектироваться средствами защиты, одной из задач которых является обеспечение минимальной продолжительности перехода угрозы атаки из разряда целевых в массовые.

Вывод. Принципиальным отличием целевой атаки является невозможность, по крайней мере с высокой вероятностью, ее детектирования, причем как собственно процесса реализации атаки, так и используемых при осуществлении атаки вредоносных компонентов (вирусов)

КСЗИ «Панцирь+» - это комплексная система защиты от целевых атак

КСЗИ «Панцирь+» - это система защиты уровня ядра ОС. Эффективная защита на уровне ядра ОС является основой безопасности любой информационной системы. Только реализовав эффективную защиту на этом уровне, уже имеет смысл реализовывать дополнительную защиту различными прикладными средствами, в том числе, решающими различные задачи детектирования!

КСЗИ «Панцирь+» позволяет в комплексе решать совокупность задач защиты от угроз целевых атак.

1. Защита от внутренних угроз (от инсайдерских атак):

- от атак со стороны интерактивных пользователей, санкционированно обрабатывающих данные в информационной системе;
- от атак со стороны привилегированных пользователей (администраторов), решающих те или иные задачи администрирования в информационной системе.

2. Защита от внешних угроз (хакерских атак).

Назначение КСЗИ «Панцирь+» в части защиты от целевых атак

В части защиты от целевых атак КСЗИ «Панцирь+» - это система защиты класса «Last frontier» - образует последний рубеж эшелонированной защиты информации.

В задачи КСЗИ «Панцирь+» входит не выявление киберугроз на ранних стадиях их возникновения, с целью противодействия осуществлению атак, что реализуется соответствующими средствами детектирования, а снижение рисков потерь от реализации атак, в предположении о том, что соответствующие угрозы не смогут быть выявлены на ранних стадиях обнаружения и атаки будут осуществлены.

Это обусловливает актуальность использования КСЗИ «Панцирь+» в качестве последнего рубежа защиты от целевых (таргетированных) атак, угрозы которых с большой вероятностью не смогут быть выявлены до момента успешной реализации подобных атак.

Основные принципы реализации защиты

Основу построения защиты составляет реализация контроля и разграничения прав доступа субъектов к объектам, с целью их локализации для решения соответствующего комплекса задач защиты информации. Способом реализации защиты является предоставление субъектам только необходимых им прав доступа к объектам, с возможностью усечения штатных потенциально опасных функций системы и приложений. Не используются какие-либо средства детектирования чего-либо, не позволяющие реализовать защиту в общем виде. Подобные средства могут применяться в дополнение к КСЗИ «Панцирь+» на защищаемых объектах информационных систем. В качестве субъекта доступа выступает сущность «пользователь, процесс», что позволяет строить эффективные разграничительную и разделительную политики доступа, учитывая при этом, что угрозу целевой атаки может нести в себе, как процесс (хакерская атака), так и легальный пользователь.

В КСЗИ «Панцирь+» реализованы следующие три основные группы механизмов защиты:

- механизмы контроля и разграничения прав доступа субъектов к статичным объектам – к объектам, присутствующим в системе на момент назначения прав доступа к ним субъектов администратором. К таким объектам относятся локальные и разделенные в сети файловые объекты, объекты реестра ОС, файловые накопители, определяемые их идентификаторами с учетом серийных номеров, сетевые объекты, локальные и сетевые принтеры и т.д. Данными механизмами реализуется разграничительная политика доступа субъектов к объектам;
- механизмы контроля и разграничения прав доступа субъектов к создаваемым объектам – к объектам, отсутствующим в системе на момент назначения прав доступа субъектов к объектам администратором, создаваемым пользователями впоследствии. К таким объектам относятся создаваемые файлы и данные, временно хранящиеся в буфере обмена. Данными механизмами реализуется разделительная политика между субъектами доступа;
- механизмы защиты от обхода разграничительной и разделительной политик доступа. Эти механизмы также реализуют контроль доступа, но уже применительно к системным объектам ОС – к сервисам олицетворения, к возможностям прямого доступа к дискам и инжектирования кода в процессы, к переменным BIOS UEFI (NV RAM) и загрузчику ОС и т.д.

КСЗИ «Панцирь+» - это сертифицированная система защиты информации

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3473

Выдан 17 декабря 2015 г.
Действителен до 17 декабря 2018 г.

Настоящий сертификат удостоверяет, что **программное обеспечение «Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows»**, разработанное и производимое ООО «НПП «Информационные технологии в бизнесе» в соответствии с техническими условиями ТУ 50 14107-021-53262993-2014, функционирующее в средах операционных систем, указанных в формуляре 643.53262993.00021-01 30, является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом, регистрации событий безопасности, ограничения программной среды, контроля целостности и защиты информационной системы, её средств и систем связи и передачи данных, соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 4 классу защищенности, «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля и техническим условий при выполнении ограничений по эксплуатации, указанных в формуляре.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Корпоративная лаборатория информационных объектов» (аттестат аккредитации от 01.10.2004 № СЗИ RU.1606.Б034.072) – техническое заключение от 30.09.2015, экспертного заключения от 06.11.2015 органа по сертификации ООО «Центр безопасности информации» (аттестат аккредитации от 09.02.2007 № СЗИ RU.117.A10.004).

Заявитель: ООО «НПП «Информационные технологии в бизнесе»
Адрес: 194044, г. Санкт-Петербург, Б. Самсониевский пр., д. 32, лит. А, оф. 2С 334
Телефон: (812) 324-2771

Контроль выполнения заявленного соответствия сертифицированной продукции и инспекционный контроль за соответствием требованиям руководящих документов и технических условий, указанных в настоящем сертификате, осуществляются испытательной лабораторией ООО «Центр безопасности информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 17 декабря 2015 г.

Реализованная технология защиты от целевых атак позволила сертифицировать КСЗИ «Панцирь+» как СЗИ НСД.

КСЗИ «Панцирь+» – это сертифицированная ФСТЭК России комплексная система защиты информации от несанкционированного доступа (СЗИ НСД), имеющая в своем составе сетевой экран.

Все механизмы защиты из состава КСЗИ «Панцирь+» сертифицированы на соответствие РД СВТ, РД МЭ, на отсутствие НДВ, большая часть ключевых механизмов защиты, в том числе от целевых атак, сертифицировано на соответствие ТУ, что обеспечивает их легитимное использование в соответствующих информационных системах: КИИ, ГИС, ИСПДн, АСУ ТП, в ИС цифровой экономики РФ .

Все механизмы защиты, решающие различные задачи, могут легитимно применяться в информационных системах, в которых требуется использование сертифицированных средств защиты.

КСЗИ «Панцирь+» реализует ролевую модель доступа

В отличие от Active Directory, КСЗИ «Панцирь+» позволяет осуществить все настройки безопасности на сервере (на сервере безопасности КСЗИ «Панцирь+»), при реализации ролевой модели доступа – не удаленно на отдельных клиентских частях системы защиты, а именно на сервере безопасности, с последующим их тиражированием в ручном, либо автоматическом режиме на все (либо отдельные) компьютеры домена.

Настройки могут осуществляться, как применительно к отдельным ролям, с их последующим тиражированием, так и применительно к информационной системе в целом. При этом настраивается одна универсальная для всех компьютеров домена разграничительная/разделительная политика доступа, автоматически (автоматизировано) распространяемая на все компьютеры домена – не требуется удаленно настраивать механизмы защиты для каждой клиентской части КСЗИ по отдельности. Это кардинально упрощает задачу администрирования системы защиты в крупномасштабной информационной системе.

Подобная возможность сервера КСЗИ «Панцирь+», как ролевого контроллера домена, обеспечивается следующими архитектурными особенностями реализации системы защиты КСЗИ «Панцирь+»:

- права (правила) доступа назначаются субъекту доступа, а не присваиваются в качестве атрибута объекту доступа;
- статичные файловые объекты, при назначении правил доступа, могут определяться переменными среды окружения;
- к создаваемым файловым объектам могут разграничиваться права доступа без учета того, в каких папках они создаются пользователями (в рамках сессии).

Защита от целевых атак со стороны интерактивных пользователей

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 риск хищения конфиденциальной информации, обеспечивая вероятность реализации подобной угрозы близкой к нулю.

Проблема защиты от хищения инсайдером (санкционированным пользователем) конфиденциальной информации особенно остра в том случае, когда на одном вычислительном средстве одному и тому же пользователю предоставляется возможность доступа к обработке как конфиденциальной, так и открытой информации. Отличие 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. Решаемая задача – предотвращение всех возможных способов перемещения данных из сессии обработки конфиденциальной информации в сессию обработки открытой информации, с целью нарушения регламента ее обработки, из которой она уже может быть похищена, что реализуется 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, и может автоматически контролироваться (по ключевых словам и фразам набираемого текста) системой оперативного контроля действий пользователей (СОК) «Панцирь+» (http://npp-itb.ru/products/sok), поставляемой в комплекте с КСЗИ.

Защита от целевых атак со стороны привилегированных пользователей

Привилегированные пользователи (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.

Механизм самозащиты КСЗИ «Панцирь+» позволяет реализовать разграничительную и разделительную политики доступа для привилегированных пользователей (ролевую модель доступа), в том числе, запретив их доступ к обрабатываемым интерактивными пользователями данным. 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.

Права администратора позволяют, используя соответствующие системные вызовы, различными способами повысить их до системных прав. Данная возможность предотвращается соответствующими механизмами защиты из состава КСЗИ «Панцирь+». При этом даже, использовав соответствующий системный процесс или службу, администратор не сможет обойти реализованные разграничительную и разделительную политики доступа, и осуществить несанкционированный доступ к обрабатываемым интерактивными пользователями данным.

Защита от целевых атак на учетные данные доменных администраторов

Вопреки бытующему мнению о том, что при реализации целевой атаки, как правило, используются уязвимости нулевого дня – выявленные ошибки программирования в программных средствах, о которых известно только злоумышленнику, 80% целевых атак предполагают взлом привилегированной учетной записи. Получить учетные данные пользователей возможно различными способами (из AD-хранилища – из файла NTDS.DIT, из локальной SAM-базы, из кэша LSA и т.д.), но 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.

Данным протоколом обеспечивается и возможность удаленного администрирования с использованием скрытых административных общих ресурсов. Так, общий ресурс ADMIN$ позволяет с правами администратора получить удаленный доступ к папке %SYSTEMROOT% другого компьютера, общий ресурс IPC$ используется при организации временных подключений, создаваемых приложениями для обмена данными с помощью именованных каналов, на практике, как правило, он применяется для удаленного администрирования серверов в сети. В этом случае по каналу уже передается «хэш» пароля администратора. Знание этого пароля администратора в доменной сети позволяет осуществить не только локальный вход с правами этого администратора на любой компьютер домена, но и с использованием скрытых административных общих ресурсов получить удаленный доступ с любого компьютера на любой компьютер домена с правами администратора.

В КСЗИ «Панцирь+» защита от угроз подобных атак реализуется двумя способами.

1. Усиление парольной защиты. Состоит в реализации дополнительного механизма идентификации и аутентификации пользователей. При этом реализовано собственное (в своей базе) защищенное хранение учетных данных пользователей. Пароль для входа в систему, отличный от пароля ОС, при удаленной аутентификации пользователей по каналу не передается - передается пароль ОС, но его хищение не позволит использованием скрытые административные общие ресурсы для удаленного администрирования.
2. Локализация рабочего места администратора. Усекается возможность удаленного администрирования в пределе только с одного компьютера в домене (учетными данными администратора можно воспользоваться только на этом компьютере).

Защита от хакерских целевых атак

Решаемые задачи защиты

Основу защиты составляет реализация разграничительной и разделительной политик доступа.

Защита от внедрения и выполнения вредоносных программ и кода - вирусов	Решается задача защиты от несанкционированного внедрения и/или выполнения исполнимых и командных файлов с правами пользователя, администратора и системы; защиты от заражения легальных исполнимых и командных файлов.
Защита данных от атак на уязвимости прикладного ПО	Решается задача защиты обрабатываемых данных и системных объектов от угроз атак, эксплуатирующих уязвимости прикладного ПО, включая фишинговые атаки и атаки вирусов шифровальщиков.
Защита от атак на повышение привилегий	Решается задача защиты от возможного получения пользователем прав администратора, которому предотвращается доступ к данным, созданным интерактивными пользователями, а администратором получение системных прав.
Защита данных от атак на уязвимости системного ПО	Решается задача защиты обрабатываемых данных, созданных интерактивными пользователями, от угроз атак, эксплуатирующих уязвимости системного ПО (системных служб и процессов).

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, что требует наличия соответствующих сигнатур и сильно влияет 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.

Вывод. Данная презентация позволяет сделать вывод о том, что КСЗИ «Панцирь+» принципиально отличается по реализуемым технологиям защиты от аналогов, предоставляя совершенно иные возможности защиты корпоративных информационных систем!

Спасибо за внимание!

Расширенная техническая презентация КСЗИ «Панцирь», иллюстрирующая способы и технические решения, реализующие комплексную защиту от целевых атак, расположена по ссылке:
http://www.npp-itb.ru/images/docs/alldocs/present.pdf

А.Ю. Щеглов, К.А. Щеглов
E-mail: info@npp-itb.spb.ru,
http://www.npp-itb.ru
Тел.:(812)324-27-71