Безопасность Windows 7. AppLocker

> Тарас Злонов, CIO-World, 13 марта 2009 года

Одной из интересных новинок в Window 7 является AppLocker - решение, которое позволяет устанавливать запрет на запуск пользователем на своём рабочем месте определённых программ.

Управление AppLocker осуществляется с помощью групповых политик (Group Policy) на сервере, в качестве которого может выступать Windows Server 2008 R2. Ранее такие задачи решались с использованием Software Restriction Policies (SRP - политики ограниченного использования программ). SRP доступны и в новой версии операционной системы, но на практике они используются довольно редко в виду трудоёмкости настройки и существующих способах их обхода.

В AppLocker предусмотрены три типа правил: правила издателя (publisher rules), правила пути (path rules) и правила хэша (File Hash Rules). Рассмотрим каждое из них более детально.

Path Rules позволяют установить запрет на запуск приложений, находящихся в заданных директориях. Например, можно разрешить пользователю использовать только те программы, которые находятся в папке `Program Files`, что в сочетании с запретом самостоятельной установки программ сделает невозможным запуск файлов, принесённых, например, из дома или скаченных из сети Интернет. В целом, наиболее эффективным использованием данного правила будет разрешение использования приложений из тех папок, для которых у пользователя нет права записи, и запрещение для тех папок, куда право записи предоставлено. При таком подходе пользователь не сможет запустить файл с рабочего стола или USB-флэш, но может запустить файл из системной папки Windows. Правила пути могут настраиваться с использованием системных и пользовательских переменных окружения (например, `%WINDIR%`) и знаков подстановок (например, `?` и `*`). Основная сложность в использовании Path Rules заключается в том, что пользователям часто требуется запускать приложения, расположенные в других местах, например, на файловом сервере. При достаточно развёрнутой инфраструктуре для отслеживания всех возможных путей размещения легитимных программ и внесения их в соответствующие правила может потребоваться значительное время.

Hash Rules основаны на использовании криптографической хэш-функции. Для разрешённого приложения вычисляется *отпечаток* его исполняемого файла и помечается как легитимный. При попытке запуска запрещённого приложения, даже переименованного пользователем с целью попытки обмана системы, например, в `CALC.EXE`, вычисленный *отпечаток* будет отличаться от сохранённого ранее и в использовании приложения пользователю будет отказано. При модификации файла в результате заражения его вирусом, установленное ограничение также не позволит запустить этот исполняемый файл. В Windows XP для этих целей использовался алгоритм MD5, а в в Windows Vista, Windows 7 и Windows Server 2008 - более новый SHA–256. Главный недостаток этого типа правил состоит в том, что новое значение хэш-функции требуется вычислять каждый раз, когда устанавливается обновление программы. Для больших программных пакетов со множеством исполняемых файлов и динамически подключаемых библиотек регулярное обновление значений хэш-функций может оказаться сложной задачей.

Publisher Rules задают ограничения на запуск программ на основе цифровой подписи, установленной разработчиком (издателем). Данный тип правил очень похож на правила сертификатов (Certifiacte Rules), которые используются в SRP. С их помощью также можно было разрешить запуск приложений и скриптов, которые подписаны, например, сертификатом Adobe, вне зависимости от их расположения и запретить запуск приложений, которые подписаны, например, Oracle. Сами сертификаты издателей при этом нужно загрузить либо локально, либо в сетевую папку. Publisher Rules позволяют выполнять настройки более гибко. Многие современные приложения, особенно от крупных вендоров, уже имеют подписи нового формата, которые можно использовать для таких настроек. Теперь у администраторов появилась возможность настраивать правила в зависимости не только от имени издателя (`Microsoft Corporation`), но и от названия самого продукта (`Internet Explorer`), имени файла (`IEXPLORE.EXE`) или версии программы (`8.0.0.0`). Последняя опция позволяет запретить или разрешить конкретные версии ПО, версии не старше определённой или наоборот - не младше заданной. При этом версия программы и версия файла в AppLocker - это разные понятия. Стоит отметить, что раннее, при использовании сертификатов старого формата, иногда компании для экономии времени подписывали у Microsoft так называемый *файл-пустышку* - то есть некий минимальный исполняемый код, который не менялся от версии к версии. При этом основной функционал программы был реализован в дополнительных библиотеках, вызываемых из подписанного файла. С введением обязательного указания версии подписываемого продукта такая хитрость разработчиков может кануть в прошлое.

Все три типа правил (пути, хэша и издателя) могут применяться к исполняемым файлам (`*.exe`), скриптам (`*.bat` , `*.cmd` , `*.vbs` , `*.js` , `*.ps1`), файлам инсталляторов (`*.msi` , `*.msp`) и системным библиотекам (`*.DLL` , `*.OCX`), охватывая тем самым практически полный список типов файлов, которые могут нанести вред системе.

В каждом создаваемом правиле есть возможность указать исключения, причём исключение может быть правилом иного типа, чем основное. Так, например, можно разрешить запускать приложения из определённой папки, но запретить при этом программы определённого издателя. Также в AppLocker есть возможность делать исключения для отдельных пользователей или групп пользователей.

Самовольный запуск пользователем программ приводит к потенциальным вирусным заражениям, дополнительной нагрузке на службу поддержки за счёт общего снижения стабильности операционной системы и сводит на нет все усилия по стандартизации корпоративного рабочего компьютера. Системные администраторы и офицеры безопасности прекрасно это понимают, но ранее предлагаемый для этого компанией Microsoft инструмент (SRP) оказался слишком не удобен в использовании. Несмотря на кажущееся отсутствие глобальных нововведений, маркетологи Microsoft приняли решение ввести новое название - AppLocker, тем самым как бы пытаясь максимально дистанцироваться от прошлых неудач. В современном мире мы не раз видели примеры, когда при отсутствии принципиально нового функционала, детально проработанный интерфейс и комфортность использования делали из очередного продукта настоящий хит. Примеры этому мы можем найти и на рынке сотовых телефоном и среди интернет браузеров, возможно, что и AppLockerскоро можно будет поставить в этот же ряд. Судить об этом можно будет, в частности, по снижению количества программ сторонних разработчиков по ограничению программ, доступных пользователю для запуска. Сейчас таких решений на рынке достаточно много.

Несмотря на изначальную ориентированность на корпоративный сегмент, AppLocker может быть интересен и домашним пользователям, заботящимся о безопасности своего компьютера. С помощью локальных настроек безопасности можно, например, разрешить запуск только доверенных приложений, снизив вероятность того же вирусного заражения. Как и многие другие новинки в Windows 7, AppLocker будет доступен только пользователям Ultimate и Enterprise версий.

Архивная копия