УДК 004.457 **Технические науки**

Митрошина Е.В., *студентка 4 курса электротехнического факультета,*
Пермский национальный исследовательский политехнический университет

APPLOCKER КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье рассматривается технология AppLocker, а именно методы создания правил, согласно трех условий, применяемые в данной технологии.

Ключевые слова: операционная система, политика безопасности, групповая политика.

Abstract. This article describes the AppLocker technology, namely methods of rules creations, according to three conditions, using in this technology.

Keywords: operating system, Security policy, group policy.

В современном мире пользователи ОС, сами того не желая, могут послужить основной причиной заражения как своего рабочего компьютера, так и целого парка компьютеров. В связи с этим в операционной системе Windows 7 появилась такая технология, как AppLocker, предназначенная для повышения безопасности, которая предотвращает запуск нежелательных приложений.

AppLocker является компонентом операционных систем Windows 7 и Windows Server 2008 R2, отвечающим за ограничение использования программного обеспечения пользователем или группой пользователей на основании определенных правил [1]. При помощи данной технологии, предоставляется возможность создавать правила, нацеленные на исполняемые файлы (файлы с расширениями *.exe, а также *.com), пакеты установщика Windows (файлы установщика Windows *.msi и файлы параметров установки *.msp), файлы заставки *.scr. Также можно создавать правила для таких сценариев, как пакетные файлы *.bat, сценарии командной строки *.cmd, сценарии PowerShell *.ps1, файлы VBScript *.vbs, а также сценарии JavaScript

*.js. И последнее, для чего можно создавать правила AppLocker – это динамические библиотеки *.dll и файлы *.ocx [3]. Недостатком является то, что AppLocker не позволяет добавлять для кастомизации правил какие-либо специфические расширения файлов. Также AppLocker позволяет назначать политики для определенных пользователей или же групп пользователей, но одно правило AppLocker возможно применить только к одной группе.

В AppLocker существуют два типа правил:

1. Разрешающие правила. В этом случае определяется файл, который разрешено пользователю или группе пользователей запускать на компьютерах.

2. Запрещающие правила**.** В этом случае определяется файл, который запрещено пользователю или группе пользователей запускать на компьютерах.

Существуют определенные условия, при которых возможно разрешить пользователям игнорировать составленные правила. Это можно сделать при помощи исключений из создаваемых правил, причем, исключения можно создавать для любого условия, независимо от того, какое вы выбирали при создании самого правила.

Очевидно, что на компьютерах пользователей может быть установлено большое количество приложений преимущественно сторонних производителей. Можно попробовать создать для каждого приложения правила вручную, однако, это утомительная процедура, при выполнении которой, можно забыть о нескольких программных продуктах. Поэтому AppLocker предусматривает помимо правил, создаваемых в ручном режиме, еще и создание правил в автоматическом режиме, что может значительно сократить время администратора, затрачиваемое на создание таких правил и, что важно, уменьшить количество пропущенных по ошибке приложений. Данная функциональная возможность крайне полезна, но у нее тоже есть свои ограничения – автоматическое создание правил позволяет создавать только разрешающие правила.

В AppLocker имеется возможность создавать правила на основании трех различных условий. Это правила для издателя, пути и хешируемых файлов [3].

В том случае, если выбирается условие «Издатель», то согласно указанным критериям будет заблокирован или разрешен доступ к приложению, основываясь на его цифровой подписи, а также на каких-либо расширенных атрибутах. К расширенным атрибутам относятся такие показатели как: наименование программного продукта, имя запускаемого файла, данные о компании-разработчике выбранного программного продукта, версия программного продукта. Правило можно использовать как для определенной версии программного продукта, так и для всех программ, выпускаемых определенной компанией. Цифровая подпись, в свою очередь, включает в себя сведения об издателе, который разработал этот программный продукт. Если же выбрать условие «Издатель», а у приложения не будет цифровой подписи, в этом случае, будет просто невозможно использовать это условие.

Следующее условие – это «Путь». Используя текущее условие, можно определять действия для приложения, согласно его физическому расположению на локальном компьютере или в сети. Здесь необходимо обратить внимание на переменные окружения, которые используются в правилах пути технологии AppLocker.

Последнее условие – это условие для хешируемого файла. В этом случае, нужно будет просто выбрать исполнительный файл какого-то приложения, а для него, при создании самого правила, будет вычислен сам хеш. Хеш представляет собой серию байтов фиксированной длины, однозначно идентифицирующую программу или файл. Они рассчитывается путем алгоритма хеширования. После того как такое правило AppLocker будет создано, в случае, если пользователь попробует открыть программу, хеш программы обязательно будет сравниваться с существующим правилом для хеша, и, естественно, будет выполнено какое-то действие. Хеш программы всегда один и тот же, независимо от расположения самой программы. Также при изменении программы хеш также меняется и, следовательно, не соответствует хешу в правиле для хеша для политик ограниченного использования программ. Поэтому, если программа обновилась, необходимо будет создать новое правило или изменять текущее.

В заключение хочется сказать, что AppLocker является необходимым инструментом, позволяющим пользователям запускать только те приложения, которые необходимы для эффективной работы. Одновременно с этим обеспечивается должный уровень защиты от неизвестного и нежелательного программного обеспечения, которое может нанести вред и повлиять на работу операционной системы.

AppLocker обеспечивает не только безопасность, но и соблюдение нормативных и эксплуатационных требований. Разрешение использования только лицензионных продуктов является необходимым требованием для соблюдения законодательства РФ, при этом автоматически снимается часть угроз, связанных с безопасностью системы.

Благодаря аудиту, присутствующему в технологии, предоставляется возможность регистрировать и анализировать различные события, которые могут быть связаны с безопасностью системы и компании в целом. А главное аудит помогает своевременно реагировать на события, которые могут предоставлять опасность для нормального функционирования системы.

Библиографический список

1. TechNet // AppLocker [Электронный ресурс]. - URL: https://technet.microsoft.com/ru-ru/library/ee424367(v=ws.11).aspx (дата обращения 23.08.2016).

2. Oszone.net // Управление доменом с помощью групповых политик [Электронный ресурс]. - URL: http://www.oszone.net/11241/Group_Policy_Domain (дата обращения 23.08.2016).

3. Планета групповой политики // Прелести технологии AppLocker [Электронный ресурс]. - URL: http://gpo-planet.com/?s=ПРЕЛЕСТИ+ТЕХНОЛОГИИ+APPLOCKER (дата обращения 23.08.2016).