НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Овезова Айна

Старший преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Гелдиева Марал

Старший преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Чарыева Дунягозел

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Аккыев Мухаммет али

Студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

В статье Social Media Impact, опубликованной ISSA Journal и написанной одним из авторов этой книги, Юрием Диогенесом, рассматривается множество случаев, когда социальные сети были основным инструментом при выполнении атаки с использованием методов социальной инженерии. Программа по обеспечению безопасности должна соответствовать кадровым и юридическим требованиям относительно того, как компания должна обрабатывать сообщения в социальных сетях, а также давать руководящие указания сотрудникам о том, как им следует вести себя в них.

Одним из сложных вопросов при определении набора руководящих принципов для сотрудников, как использовать социальные сети, является определение надлежащего делового поведения. Дисциплинарные меры в отношении работников, которые пересекают эту границу, должны быть очень четкими. В октябре 2017 г., сразу после массовых расстрелов в Лас-Вегасе, вице-президент CBS сделала комментарий, предположив, что «жертвы Вегаса не заслужи ли сочувствия, потому что поклонники кантри часто являются республиканцами». Результат этого онлайн-комментария был прост: она была уволена за нарушение стандартов поведения компании. Хотя для CBS важно было быстро извиниться за ее поведение и продемонстрировать соблюдение политики путем увольнения сотрудника, компания все же пострадала от комментариев этого человека.

При наличии политической напряженности в мире и свободы, которую социальные сети дают людям, чтобы выразить свои мысли, подобные ситуации возникают каждый день. В августе 2017 г. профессор Флориды был уволен из-за сообщение в Twitter, в котором говорилось, что Техас заслужил ураган Харви, после того как проголосовал за Трампа.

Это еще один пример того, как сотрудник использует свой личный аккаунт в Twitter для онлайн-декламаций, приводящих к плохим последствиям. Зачастую компании принимают решение уволить сотрудника, который плохо себя ведет в интернете, основываясь на кодексе поведения. Например, если вы прочитаете раздел «Внешние коммуникации» в Кодексе поведения Google, то увидите, какие рекомендации дает Google относительно публичного раскрытия информации.

Тренинг по безопасности

Тренинг по безопасности должен проводиться для всех сотрудников. В него необходимо включать рассказы о новых методах атак и соображения по этому поводу. Многие компании проводят такое обучение в режиме онлайн через внутреннюю сеть компании. Если тренинг хорошо продуман, богат визуальными эффектами и в конце содержит вопросы для самопроверки, он может быть очень результативен. В идеале тренинг по безопасности должен содержать:

-примеры из реальной жизни. Пользователям будет легче запомнить что-либо, если вы покажете реальный сценарий. Например, говорить о фишинговых письмах, не показывая, как они выглядят и как их визуально идентифицировать, не очень эффективно;

-практика. Хорошо написанный текст и богатые визуальные элементы – важные атрибуты учебных материалов, но вы должны представить пользователю практические сценарии. Позвольте ему взаимодействовать с компьютером, чтобы выявить целевой фишинг или фальшивую кампанию в социальных сетях.

В конце тренинга все пользователи должны подтвердить, что они успешно прошли его и знают не только об угрозах безопасности и контрмерах, описанных в тренинге, но и о последствиях несоблюдения политики безопасности компании.

Использование политики

Когда вы закончите создавать свою политику безопасности, наступит время ее применения, которое осуществляется с использованием различных технологий в соответствии с потребностями компании. В идеале должна быть схема архитектуры вашей сети, чтобы в полной мере понять, какие у вас есть ключевые точки, т. е. какие серверы у вас имеются, как идут потоки информации, где хранится информация, у кого есть и у кого должен быть доступ к данным, а также каковы различные точки входа в вашу сеть.

Многие компании не в состоянии полностью реализовать политику безопасности, потому что они думают о ее применении только на конечных точках и серверах.

А как насчет сетевых устройств? Вот почему вам нужен целостный подход к каждому компоненту, активному в сети, включая коммутаторы, принтеры и IoT-устройства.

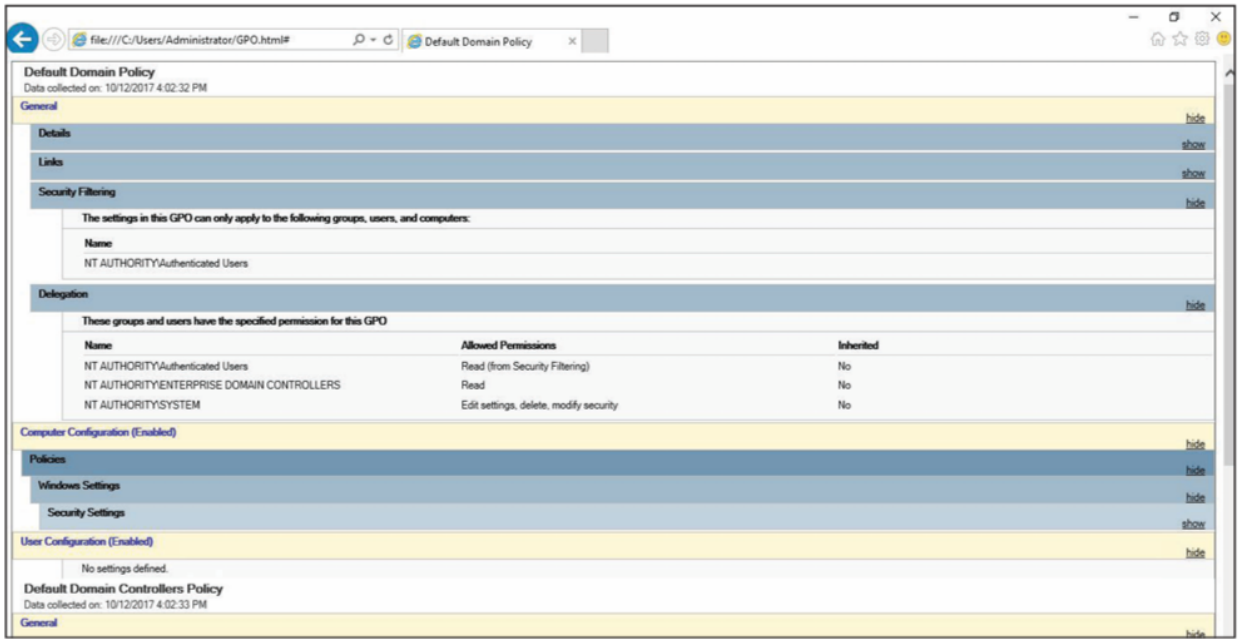
Если в вашей компании есть служба каталогов Microsoft Active Directory, вы должны использовать объект групповой политики (GPO) для развертывания своей политики безопасности. Все политики должны быть развернуты в соответствии с политикой безопасности вашей компании. Если у разных отделов разные потребности, вы можете сегментировать свое развертывание, используя организационные единицы (OU), и назначать политики для каждой отдельной единицы.

Например, если серверам, которые относятся к отделу кадров, требуется другой набор политик, вы должны переместить эти серверы в единицу HR и назначить для нее специальную политику.

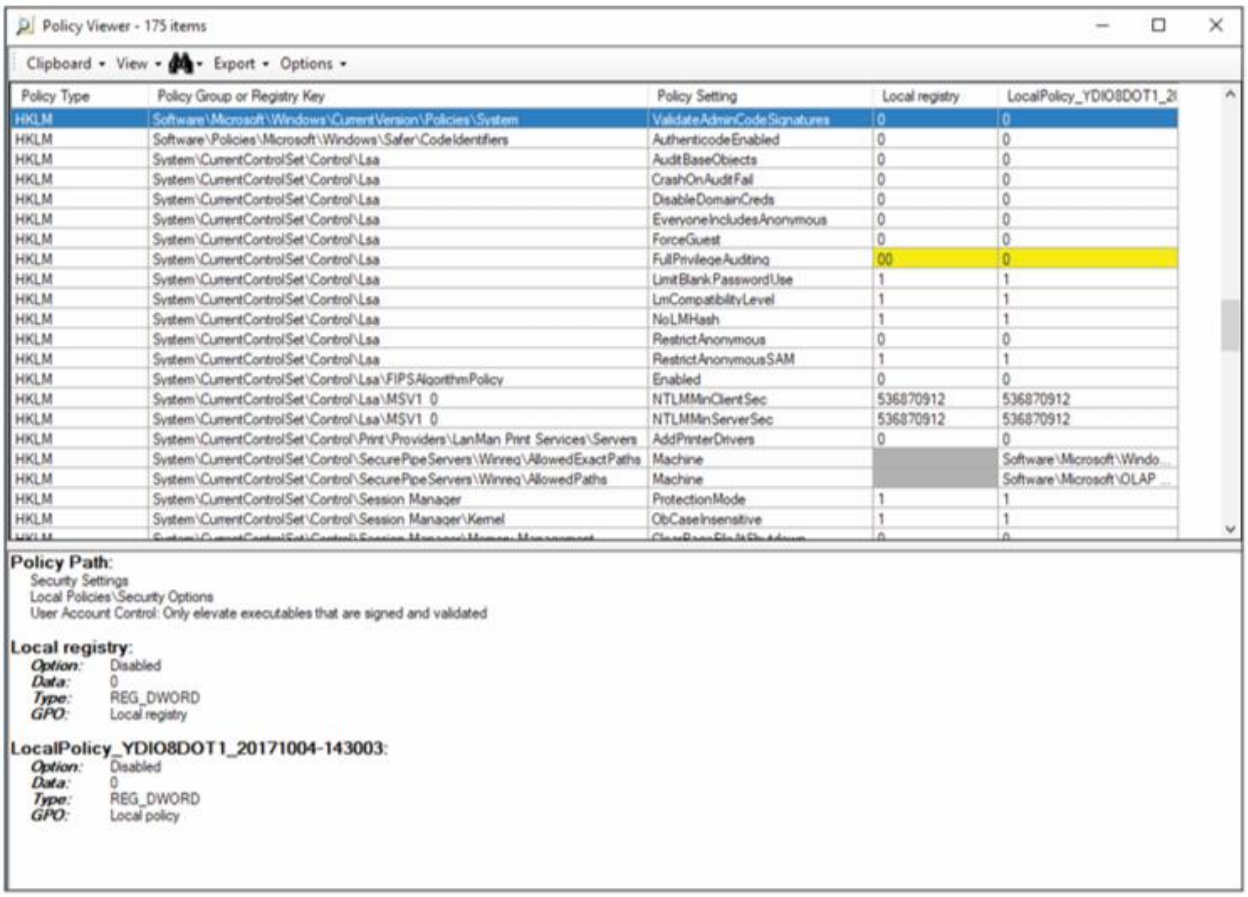
Если вы не уверены в текущем состоянии своих политик безопасности, вам следует выполнить начальную оценку с помощью команды PowerShell Get GPOReport, чтобы экспортировать все политики в HTML-файл. Убедитесь, что вы запустили следующую команду с контроллера домена:

PS C:> Import-Module GroupPolicy

PS C:> Get-GPOReport -All -ReportType HTML -Path .GPO.html



Также рекомендуется выполнить резервное копирование текущей конфигурации и сделать копию этого отчета, прежде чем вносить какие-либо изменения в текущие групповые политики. Еще один инструмент, который вы также можете использовать для выполнения этой оценки, – это Policy Viewer, входящий в состав Microsoft Security Compliance Toolkit, доступный на странице **https://www.microsoft.com/en-us/download/details.aspx?id=55319**



Преимущество этого инструмента в том, что он просматривает не только объекты групповой политики, но и проверяет корреляцию политики со значениями ключей реестра.

Если политика безопасности вашей организации требует, чтобы на компьютере пользователя разрешалось запускать только лицензионное программное обеспечение, необходимо запретить пользователям запускать нелицензионные программы, а также ограничить использование лицензионного программного обеспечения, которое не авторизовано IT-отделом. Соблюдение политики гарантирует, что в системе будут работать только авторизованные приложения.

При планировании соблюдения политик для приложений нужно создать список всех приложений, которые разрешено использовать в компании. Основываясь на этом списке, вы должны изучить детали этих приложений, задав следующие вопросы:

-Каков путь установки для каждого приложения?

-Какова политика обновлений у поставщика для этих приложений?

-Какие исполняемые файлы используют эти приложения?

Чем больше информации вы можете получить о самом приложении, тем более осязаемыми будут ваши данные, чтобы определить, было приложение подделано или нет. Для систем Windows следует запланировать использование AppLocker и указать, какие приложения разрешено запускать на локальном компьютере.

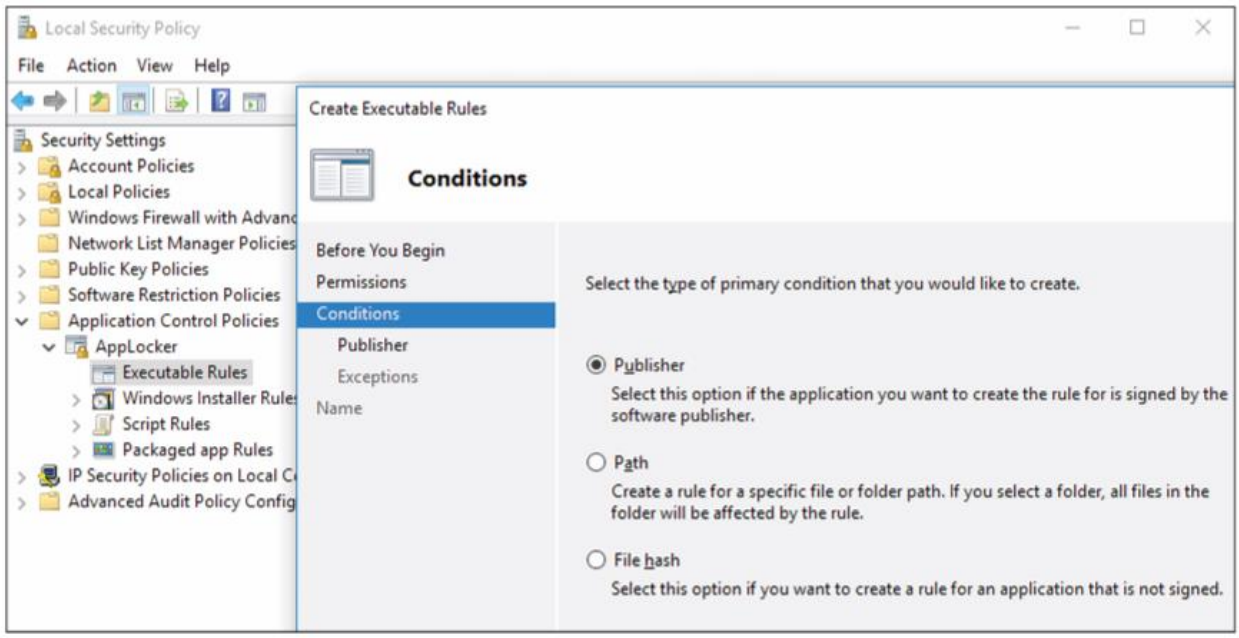
В AppLocker есть три типа условий для оценки приложения:

-издатель – следует использовать, если вы хотите создать правило, которое будет применяться к приложениям, подписанным поставщиком программного обеспечения;

-путь – следует использовать, если вы хотите создать правило, которое будет применяться к приложениям в зависимости от папки, в которую оно установлено;

-хеш файла – следует использовать, если вы хотите создать правило, которое будет применяться к приложениям, которые не подписаны поставщиком программного обеспечения.

Эти параметры появятся на странице Conditions (Условия) при запуске мастера создания исполняемых правил



Какой вариант вы выберете, будет зависеть от ваших потребностей, но эти три варианта должны охватывать большинство сценариев развертывания. Имейте в виду, что в зависимости от того, какому варианту вы отдадите предпочтение, на следующей странице появится новый набор вопросов. Убедитесь, что вы ознакомились с документацией по AppLocker на странице **https://docs. microsoft.com/ru-ru/windows/security/threat-protection/windows-defender-applica tion-control/applocker/applocker-overview.**