Инструменты для обеспечения безопасности в облачных сервисах на примере Microsoft Office 365

Microsoft Office 365

Microsoft Office 365 – это программный продукт, объединяющий набор веб-сервисов. Распространение происходит на основе подписки по схеме «программное обеспечение + услуги». Набор предоставляет доступ к различным программам и услугам на основе платформы Microsoft Office, электронной почте бизнес-класса, функционалу для общения и управления документами. [1]

Рисунок 1 – Логотип Microsoft Office 365

Office 365 в первую очередь разрабатывался для обеспечения почтового хостинга, доступа к корпоративным социальным сетям и облачному хранилищу данных для бизнеса.

Для того, чтобы предоставлять услуги для разных типов бизнеса, а также для отдельных пользователей, которые хотят использовать пакет ПО Office на основе подписки, с выходом Microsoft Office 2013 было осуществлено расширение Office 365. [2]

Таким образом Microsoft Office 365 является гибким, мобильным и экономичным инструментом, но при работе с «облаком» остро встает вопрос безопасности данных.

Рассмотрим, какие встроенные функции помогут сделать работу с данным программным продуктом более безопасной для данных.

Политика безопасности

В Microsoft Office 365 имеется возможность использовать политику безопасности и ограничение времени действия пароля, чтобы обезопасить данные и ограничить доступ к приложениям. Также имеются различные настройки сроков обновления паролей в зависимости от профилей пользователей. Для пользователей облачных сервисов по умолчанию пароли теряют актуальность спустя 90. Для пользователей облачных сервисов имеется возможность сброса пароля в режиме самообслуживания.

Предлагается несколько способов аутентификации при сбросе пароля – через офисный телефон, мобильный телефон, e-mail и секретные вопросы.

Предупреждение потерь данных (DLP)

Стратегия предупреждения потерь данных гарантирует сохранность и конфиденциальных персональных данных от несанкционированной загрузки, распространения или отправки по электронной почте. DLP доступна в SharePoint Online и Exchange, и может быть интегрирована с Enterprise Search. Вместе с этим можно создавать политики для ограничения сохранения контента в различных местах, таких как One Drive for Business и SharePoint Online.

Рисунок 2 –Логотип Microsoft Share Point

При включении DLP для работы в режиме тестовой проверки он предоставит отчет о фактах несогласованной загрузки и хранения данных, нарушающих политику безопасности.

Рисунок 3 –Логотип One Drive for Business

Управление правами

Управление правами позволяет защищать документы и электронную почту при помощи использования шифрования и связанной политики доступа.

Документы могут быть использованы только определенными пользователями для определенных целей. Можно установить правила соответствия содержания и создать настройки оффлайн-доступа, также как и установить политики на уровне документа, которые, например, не позволят неавторизованному пользователю открыть документ в формате Word, сохраненный на диск. Эта опция требует лицензии E3 или лицензии на управление правами в Azure.

Рисунок 4 –Логотип Azure

Шифрование сообщений в Office 365

Шифрование сообщений в Office 365 требует ввода пароля и логина для чтения и ответа на письма. Оно осуществляется при помощи пароля однократного доступа для доступа к электронному письму. Шифрование сообщений доступно в E3 Office 365.

Управление мобильными устройствами (MDM)

Управление мобильными устройствами позволяет защищать данные на устройствах пользователей. MDM позволяет установить условия доступа, разграничить политики для различных пользователей, управлять мобильными устройствами и удалять с них данные при необходимости, частично или полностью. MDM свободно предлагается в пакетах коммерческой подписки на Office 365 с мая 2015 года.

Многофакторная аутентификация

Многофакторная аутентификация требует не только имя пользователя и пароль для доступа в Office 365. Она может быть устанавливаться для каждого пользователя индивидуально. Пользователи, помимо привычных логина и пароля, получают звонок на телефон или текстовое сообщение. Ответ на звонок или ввод полученного кода доступа в браузере обеспечивает аутентификацию с повышенным уровнем безопасности. Система может включаться в зависимости от IP-адреса, при этом запрашивая дополнительный код только при доступе из публичных сетей и деактивируясь при работе в офисе. Многофакторная аутентификация является бесплатной опцией в Office 365.

Расширенная защита от угроз

Exchange Online Protection защищает все почтовые ящики Exchange Online в составе подписки. Расширенная защита от угроз будет доступна в качестве дополнительной опции для борьбы с такими серьезными проблемами, как фишинг от лица доверенных источников и атаки вредоносного ПО через уязвимости приложений.

Рисунок 5 –Логотип Exchange Online

Безопасность клиентских устройств

Также решен вопрос безопасности клиентских устройств, которые имеют доступ в Office 365.

Обновления для решения проблем ИБ своевременно установлены.

Используя Active Directory Federation Services имеется возможность установить политики безопасности, которые ограничивают пользователей от входа в систему с определенных IP-адресов.

Развертывание клиента Office

Данный способ обеспечения безопасности обеспечивает актуальность клиентской версии Office через установку актуальных обновлений.

Пользователи имеют возможность гибкой настройки обновлений через определенные временные интервалы. Можно контролировать ситуацию через основанный на XML процесс Click2Run, доступный только в планах подписки Office 365 Pro Plus.

Совместное использование контента

Портал администратора предоставляет возможность включения или ограничения совместного использования контента. Имеется возможность контролировать использование контента в Office 365, включая сайты, календарь, Skype for Business и другие приложения. Присутствуют отчеты, демонстрирующие настройки совместного доступа к контенту. Администратор может изменить настройки непосредственно из консоли управления, без входа в настройки приложения.

Литература:

1. Работа с Office на любом устройстве // https://products.office.com/ru-ru/?legRedir=default&CorrelationId=22c50f61-8ff6-4550-a2ff-c06aeabc30... (дата обращения 10.06.2015).
2. Microsoft Office 2013 против Microsoft Office 365 // http://www.pcworld.com/article/2026703/office-365-vs-office-2013-should-you-rent-or-own-.html (дата обращения 14.06.2015).