АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В WINDOWS AZURE

Ганзенко В.В., Добрынин И.С.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. ТКС, тел. (057) 702- 55- 92 ,
E-mail: marunich.v.v@gmail.com

Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources .This may take the form of web-based tools or applications that users can access and use through a web browser as if they were programs installed locally on their own computers. Windows Azure, as an application hosting platform, must provide confidentiality, integrity, and availability of customer data. It must also provide transparent accountability to allow customers and their agents to track administration of services, by themselves and by Microsoft.

Отличительной особенностью облаков является: высокая пропускная способность, более дешевое хранение и надежная технология виртуализации, сделавшая идею программного обеспечения как службы реальностью. Облачные вычисления обеспечивает масштабируемые, гибкие системы с оплатой текущих расходов, соответствующие требованиям поколения «больших результатов с меньшими затратами», но безопасность остается критически важной проблемой. Обеспечение безопасности в Windows Azure состоит из трех основных компонентов: конфиденциальности, целостности и доступности, также как и в любой распределенной сети. В данном докладе подробно будут рассмотрены механизмы защиты информации для приложений и служб в Windows Azure.

Предложено несколько механизмов защиты информации для приложений и служб, размещенных в Windows Azure.

1. Владение учетной записью.

Портал для клиентов Майкрософт (MOCP) позволяет управлять учетными записями и биллингом в Windows Azure. На портале MOCP можно подписаться на службы Windows Azure, а также дополнительные службы, такие как SQL Azure, и создать новые экземпляры подписок. Подписки — это «граница биллинга» для служб Windows Azure. Для всех приложений, которым необходима особая структура биллинга, требуются отдельные подписки. Для каждой подписки определяются учетные записи «владельца учетной записи» и «администратора службы». Эти учетные записи связаны с учетными записями Windows Live ID. Владелец учетной записи самостоятельно отвечает за управление подпиской и биллингом на портале MOCP.

Акцентировано внимание на создании отдельных учетных записей для этих ролей. Эти учетные записи независимы от отдельных учетных записей. Для идентификации пользователя в системе необходимо использовать персональную учетную запись Windows Live ID в качестве учетной записи владельца или администратора учетной записи. Для создания уникальной учетной записи можно использовать схему именования (например, AO[уникальный идентификатор]@uib.ua для владельца учетной записи и AA[уникальный идентификатор]@uib.ua для администраторов учетной записи) с паролями, которыми можно управлять и восстанавливать при необходимости, на централизованном уровне. После создания подписи администраторы учетных записей могут управлять размещенными службами на портале управления Windows Azure. Для этого используются учетные данные учетной записи администратора службы.

2. Использование сертификатов.

Существует два вида сертификатов, использующихся в защите приложений и служб: сертификаты служб и сертификаты управления.

Сертификаты служб — это традиционные сертификаты SSL, используемые для защиты связи конечных точек. Сертификаты служб используются для рабочих развертыва-

ний сред, выпускаемых доверенным корневым центром сертификации (CA). Поэтому они отдельно приобретаются у стороннего поставщика.

Имя сертификата SSL должно соответствовать имени домена веб-сайта. Для этого нужна запись DNS CNAME для сопоставления app.cloud.net (имя домена для приложения, предоставленное Windows Azure) с www.yourcompany.com. Для целей обеспечения безопасности нельзя приобрести сопоставление сертификатов с app.cloud.net. Только корпорация Майкрософт может выпускать сертификаты для cloud.net, хотя для целей разработки можно создавать собственные само подписывающиеся сертификаты.

Сертификаты управления — другой тип сертификатов, использующихся Windows Azure. Средства Windows Azure для Microsoft Visual Studio используют сертификаты управления для проверки подлинности разработчиков для развертывания Windows Azure. Средство командной строки CSUpload также использует сертификаты управления для развертывания ролей образов виртуальных машин, выполняющих запросы Windows Azure Service Management REST API.

Одной из основных проблем организации является изменение учетной записи пользователя, например, когда сотрудник перестает работать на данном предприятии. Для того чтобы закрыть доступ пользователю к ресурсам или просто внести изменения в учетную запись сотрудника необходимо следовать следующим правилам.

Правило 1 — восстановление паролей для всех учетных записей администраторов служб, к которым имел доступ бывший сотрудник. Если установлены уникальные и независимые идентификаторы владельца учетной записи и администратора службы с возможностью централизованного управления, это упростит данный процесс. Если невозможно восстановить пароль для учетной записи администратора службы, можно войти в систему MOCP как владелец учетной записи, обновить учетную запись, указанную как запись администратора службы. Также необходимо удалить все учетные записи, указанные для дополнительных администраторов на портале управления Windows Azure.

Правило 2 — повторный выпуск всех необходимых сертификатов управления. Эти сертификаты предоставляют средства проверки подлинности для размещенной службы через API Visual Studio и Windows Azure. Поэтому им нельзя больше доверять после того, как сотрудник прекращает трудовые отношения.

Выше перечисленные механизмы защиты информации в Windows Azure, позволят предотвратить различные утечки информации, как от доверенных сотрудников, так и от лиц с которыми заключены деловые отношения. Также уменьшить риск зависимости бизнеса от ИТ - структуры.

Литература:

1. Cloud computing [Электронный ресурс] / En.wikipedia.org – Режим доступа URL: http://en.wikipedia.org/wiki/Cloud_computing – 20.08.2011 – Загл.с экрана.

2. Windows Azure. Общие сведения об управлении учетными записями безопасности в Windows Azure [Электронный ресурс] / Oszone.net. Джошуа Хоффман – Режим доступа URL: http://www.oszone.net/15725/Windows-Azure - 19.07.2011 – Загл. с экрана.

3.Windows Azure Security Overview [Электронный ресурс] / Globalfoundationservices.com. Charlie Kaufman and Ramanathan Venkatapathy – Режим доступа URL:http://www.globalfoundationservices.com/security/documents/WindowsAzureSecurityOverview1_0Aug2010.pdf - 01.08.2011 - Загл. с экрана.