БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Риски, возникающие при использовании облачных сервисов

Облака это круто

Наиболее важные преимущества

Скорость выделения ресурсов

Эффективность использования

Прозрачность

Риск №1 Конфиденциальность данных

Угрозы	Источник
Несанкционированный доступ к базе данных при использовании базы данных как сервиса	Провайдер
Несанкционированный доступ к виртуальным серверам	Провайдер
Несанкционированный доступ к виртуальным серверам	Провайдер
Несанкционированный доступ к данным в опубликованной базе данных	Внешний нарушитель
Несанкционированный доступ к облачной инфраструктуре	Внешний нарушитель

Риск №1 Конфиденциальность данных

Рекомендация
Шифровать конфиденциальные данные, хранимые в базе данных
Шифровать данные при передаче. Проверять ли сертификаты?
Удалять системных пользователей и/или пакеты, созданные провайдером, с виртуальных серверов.
Запретить, на уровне сетевых сегментов, публичный доступ к базам данных
Мониторинг управленческих событий на уровне облака
Обязательное использование МФА для доступа к облаку
Контроль целостности контейнеров

Риск №2 Доступность сервиса

Чем больше мы доверяем облаку, тем больше становимся зависимы от него.

Угрозы	Источник
Ограничение доступа из-за санкционных ограничений	Провайдер
Любой иной отказ в предоставлении услуги со стороны провайдера	Провайдер
Технический сбой на оборудовании провайдера	Провайдер
Несанкционированный доступ к облачной инфраструктуре	Внешний нарушитель

Риск №2 Доступность сервиса

Чем больше мы доверяем облаку, тем больше становимся зависимы от него.

Рекомендации
Обязательное резерв данных, исходного кода приложений и описания инфраструктуры в месте, вместе не зависящем от текущего провайдера облачных сервисов
Обязательное использование MFA
Запрет на использование рутового аккаунта для целей администрирования
Мониторинг сообщений от провайдера о техническом обслуживании или деградации оборудования
Отдельные OU для администраторов, безопасников, тестировщиков, разработчиков и основной инфраструктуры

Риск №3 Избыточная стоимость

Чем больше мы доверяем облаку, тем больше становимся зависимы от него.

Угрозы	Источник
Бесконечное масштабирование сервисов во время ддос-атаки	Внешний нарушитель
Любой иной отказ в предоставлении услуги со стороны провайдера	Провайдер
Технический сбой на оборудовании провайдера	Провайдер
Несанкционированный доступ к облачной инфраструктуре	Внешний нарушитель

Риск №3 Избыточная стоимость

Чем больше мы доверяем облаку, тем больше становимся зависимы от него.

Рекомендации
Необходимо лимитировать масштабируемые сервисы
Необходимо использовать средства защиты от атак на прикладном уровне
Необходимо контролировать загрузку виртуальных серверов

Риск №4 Несанкционированное изменение ПО

Чем больше мы доверяем облаку, тем больше становимся зависимы от него.

Угрозы	Источник
Неконтролируемое внесение изменений при сборке контейнеров	Провайдер, Внешний нарушитель
Неконтролируемое внесение изменений при компиляции прикладного ПО	Провайдер, Внешний нарушитель

Риск №4 Несанкционированное изменение ПО

Чем больше мы доверяем облаку, тем больше становимся зависимы от него.

Рекомендации
Необходимо полностью контролировать репозиторий исходного кода
Необходимо полностью контролировать регистр контейнеров
Необходимо контролировать целостность кода

Итог. Рекомендации

Рекомендация
Необходимо шифровать данные при их хранении и передаче.
Контролировать доступ провайдера к используемым сервисам.
Запретить публичный доступ к критичным сервисам, серверам и БД
Мониторинг управленческих событий на уровне облака
Обязательное использование МФА для доступа к облаку, и запрет на администрирование из под рутовой учетки. Разделение функционала на уровне OU
Обязательное резерв данных, исходного кода и описания инфраструктуры в месте, вместе не зависящем от текущего провайдера облачных сервисов
Мониторинг сообщений от провайдера о техническом обслуживании или деградации оборудования
Кимитировать масштабируемые сервисы и контролировать загрузку серверов
Необходимо использовать средства защиты от атак на прикладном уровне
Хранить исходный код, приложения и контейнеры в контролируемом месте и обеспечивать контроль целостности при использовании

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!