БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Рекомендации по минимизации рисков, возникающих при миграции в облако

Зачем мигрировать в облако

Наиболее важные преимущества

- Скорость
- Время
- Ресурсы
- Затраты

Угрозы, возникающие при миграции

Угрозы	Источник
Несанкционированный доступ к ресурсам со стороны провайдера	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

продолжение ...

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

и еще

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

Как снизить возможные риски?

Прежде всего не нужно доверять третьим лицам то, что имеет критической влияние на бизнес-процессы в компании.

Не стоит лишать себя возможности восстановить работоспособность сервиса, даже если облако вдруг станет недоступно.

Если нет собственных ресурсов, то допускается аренда ресурсов в другом облаке для хранения резервных копий данных и приложений

Что можно и нужно доверить облаку

Облако создано для быстрого и эффективного выделения ресурсов для приложений.

Как снизить возможные риски?

Необходимо контролировать все, что происходит в облаке.

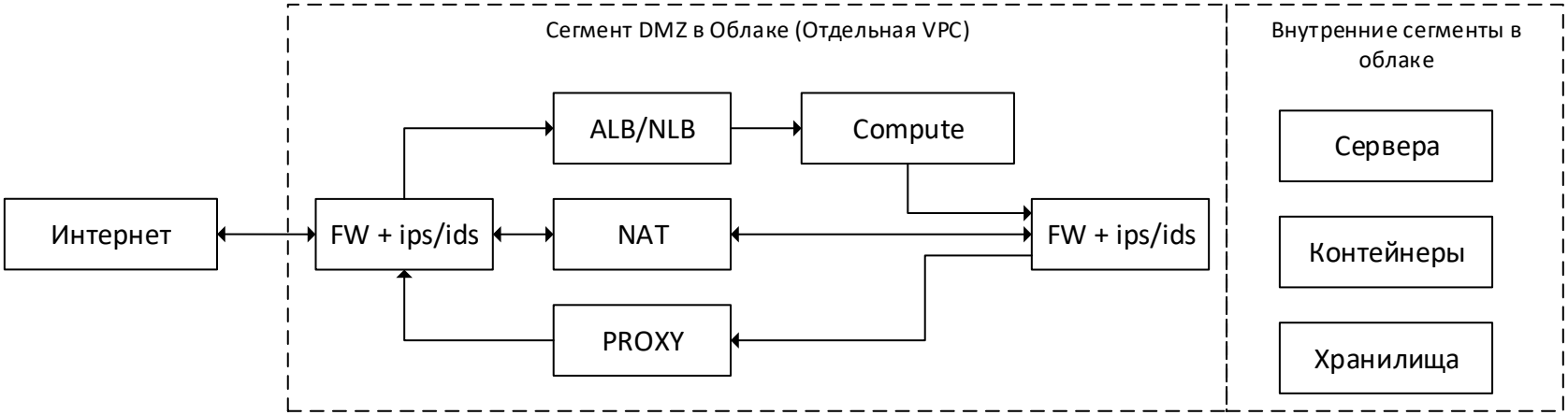
Вы должны знать о том, что кто-то пытается атаковать ваши ресурсы.

Также, использование облачной инфраструктуры не должно снижать общую защищенность ресурсов компании и не должно создавать дополнительные возможности для осуществления атак.

Контроль за облаком

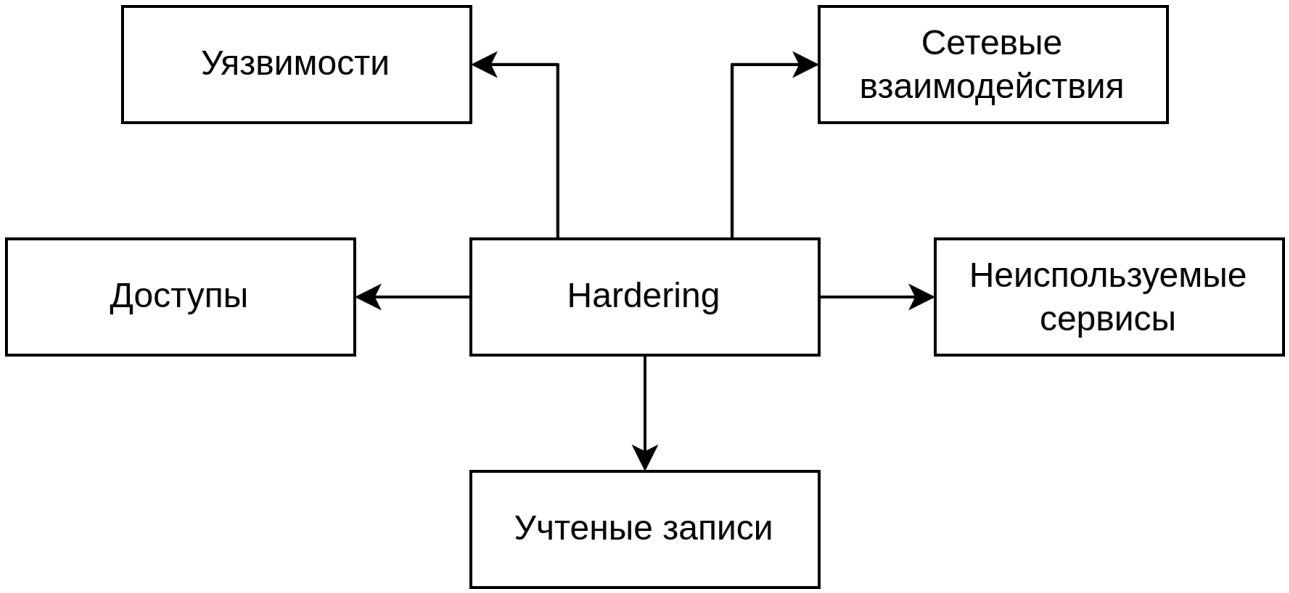
Нужно ли формировать ДМЗ в облаке

Ответ простой – да.
Цель - контроль

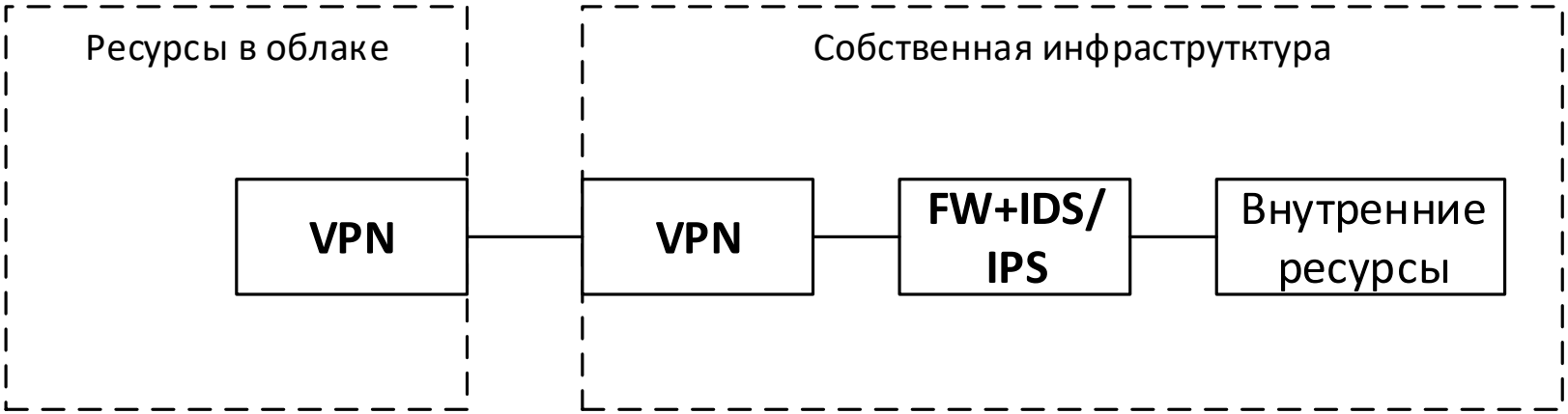


Как снизить возможные риски?

System hardering



Взаимодействие с облачной инфраструктурой



Итог. Полезные рекомендации

Рекомендация
Необходимо защищать данные при их хранении и передаче.
Контролировать все, что происходит в облаке
Запретить публичный доступ к критичным сервисам, серверам и БД. ДМЗ
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
Использование средств защиты для сохранения уровня защищанности
Хранить исходный код, приложения и контейнеры в контролируемом месте и обеспечивать контроль целостности при использовании
Hardering

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!