Virtualization Security Group Russia

группа специалистов

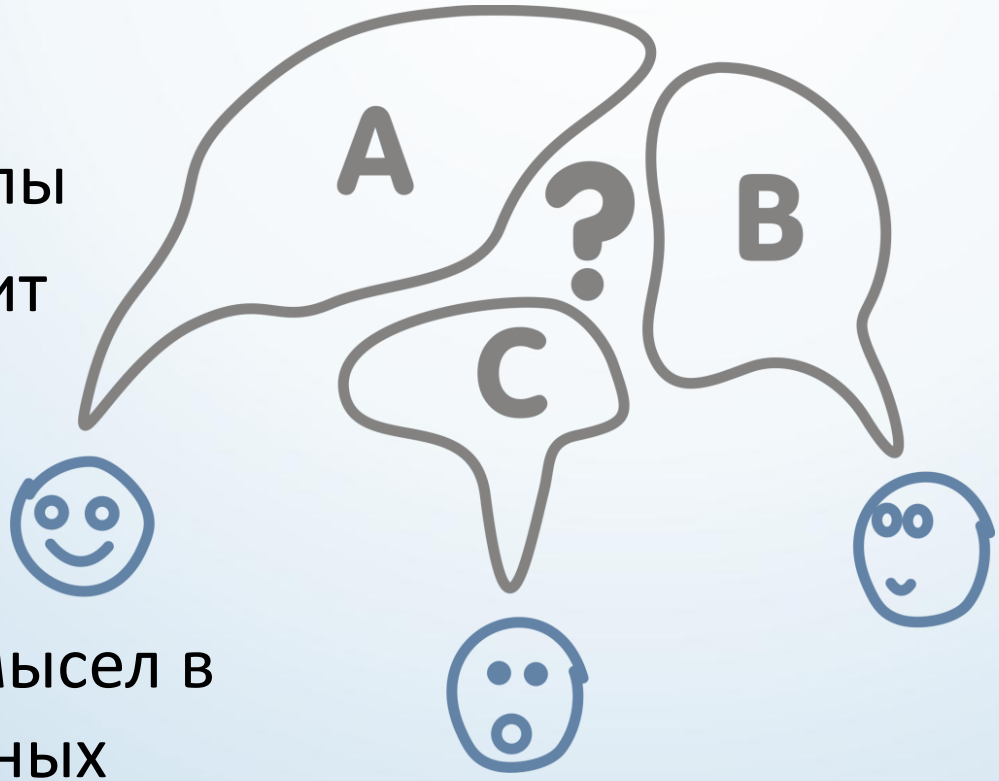
Мифы виртуализации. Самые распространенные заблуждения и стереотипы относительно обеспечения информационной безопасности инфраструктур виртуализации

Мария Сидорова, *Главный редактор VirtualizationSecurityGroup.ru*

Вместо предисловия

Virtualization Security Group Russia
группа специалистов

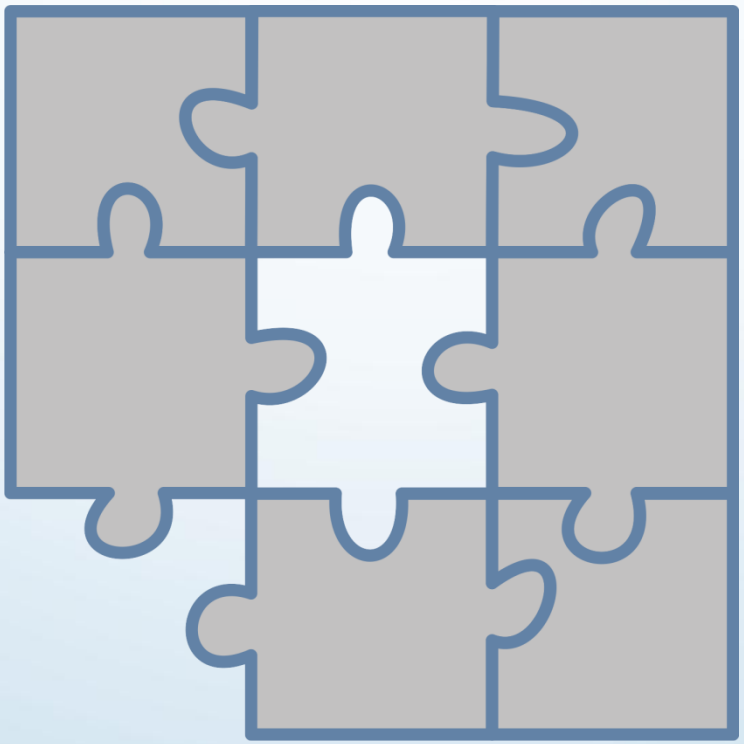
- Специалисты часто принимают решения, опираясь на стереотипы
- Развенчать миф, значит понять какие и чьи потребности он удовлетворяет
- Что, правда, а что вымысел в самых распространенных мифах о виртуализации



Миф 1. Традиционных средств защиты – достаточно

Virtualization Security Group Russia
группа специалистов

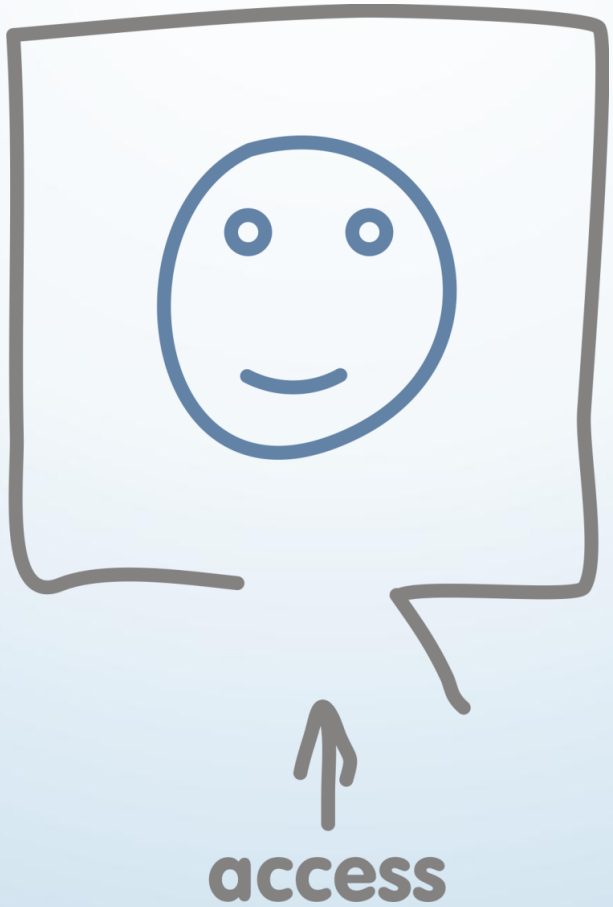
- Новые векторы угроз
- Высокая динамика среды
- Невозможность применять некоторые привычные средства обеспечения информационной безопасности в том виде, в котором они существуют



Миф 2. Взломать гипервизор – невозможно

Virtualization Security Group Russia
группа специалистов

- Ключевой элемент архитектуры сред виртуализации
- Существуют методики компрометации
- На сегодняшний день не было случаев масштабных проблем в реальных информационных системах связанных с компрометацией гипервизора

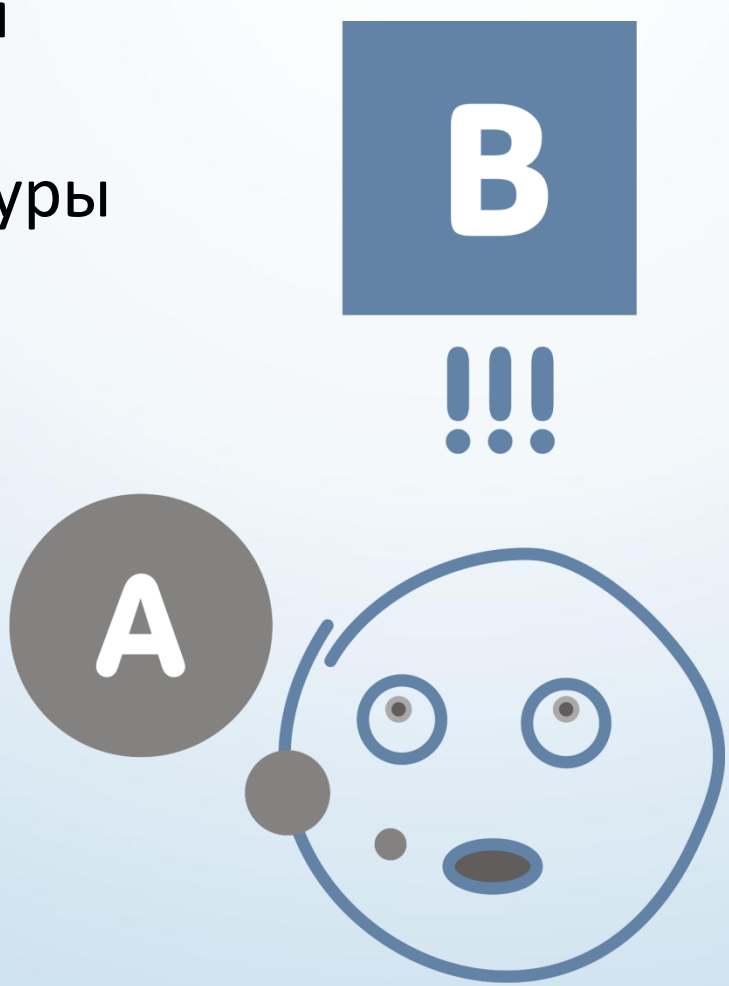


Миф 3. Решения виртуализации сами по себе позволяют повысить уровень обеспечения информационной безопасности

Virtualization Security Group Russia
группа специалистов

- Сама по себе виртуализация не повышает уровень защищенности инфраструктуры
- VMsafe – технология, позволяющая

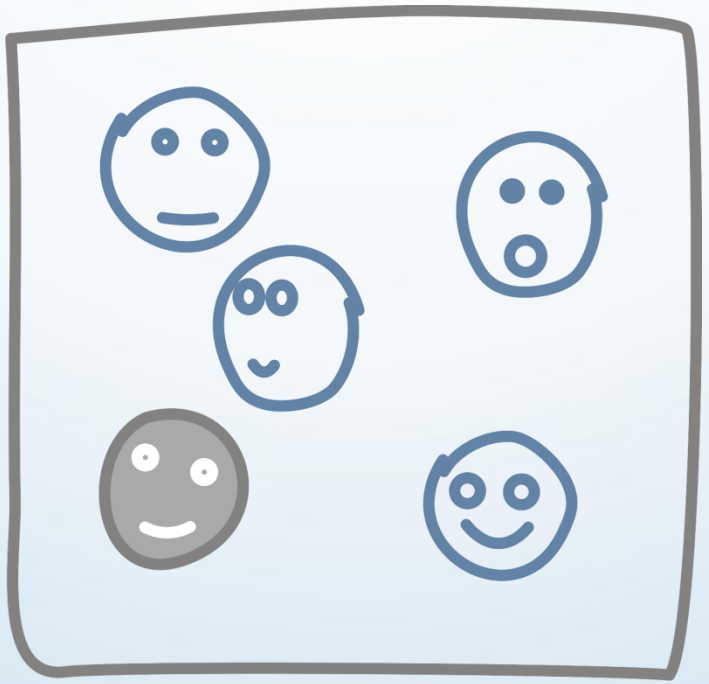
  сторонним разработчикам получить доступ к гипервизору



Миф 4. Достаточно защищать только сервера виртуализации, они защитят виртуальные машины

Virtualization Security Group Russia
группа специалистов

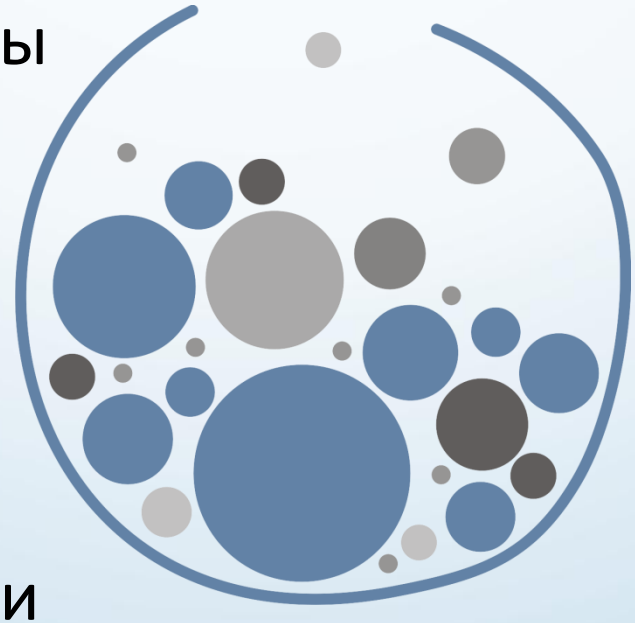
- Виртуальные машины подвержены абсолютно тем же атакам, что и машины физические
- Функции по защите выполняет такая же виртуальная машина, как и защищаемые (Virtual Appliance)
- Эффективная защита должна быть многоуровневой



Миф 5. Использование систем хранения данных безопасно по умолчанию

Virtualization Security Group Russia
группа специалистов

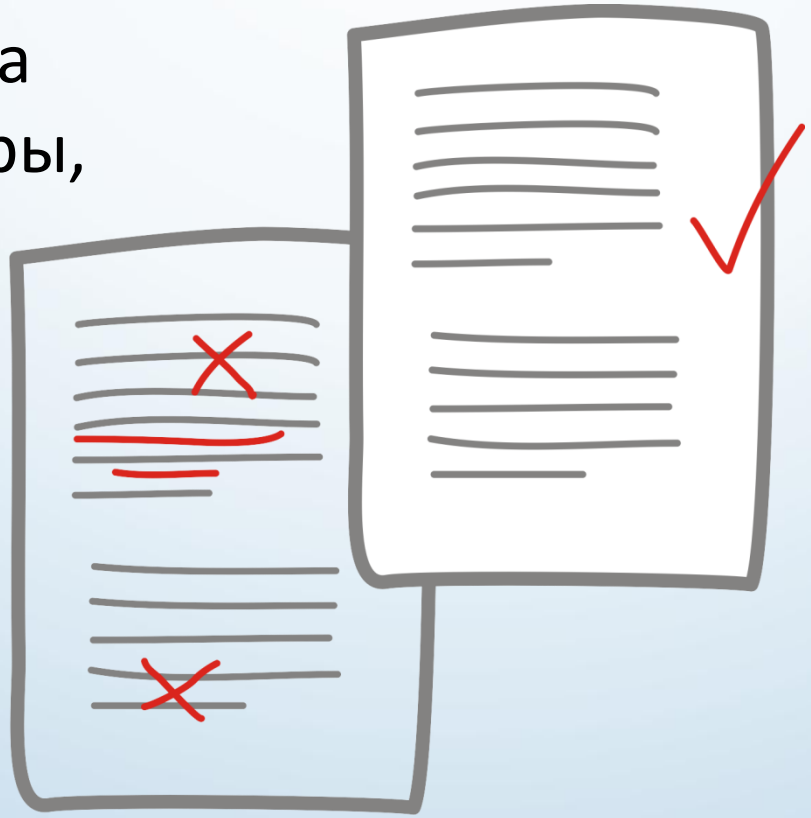
- Поскольку виртуальная машина представляет собой совокупность файлов, возникает риск того, что эти файлы могут быть скопированы либо подменены
- После внедрения серверной виртуализации сразу несколько виртуальных машин находятся в одном разделе в целях обеспечения "горячей" миграции и отказоустойчивости



Миф 6. Инструкции и регламенты реагирования на инциденты для виртуальных сред остаются такими же, как и для физических инфраструктур

Virtualization Security Group Russia
группа специалистов

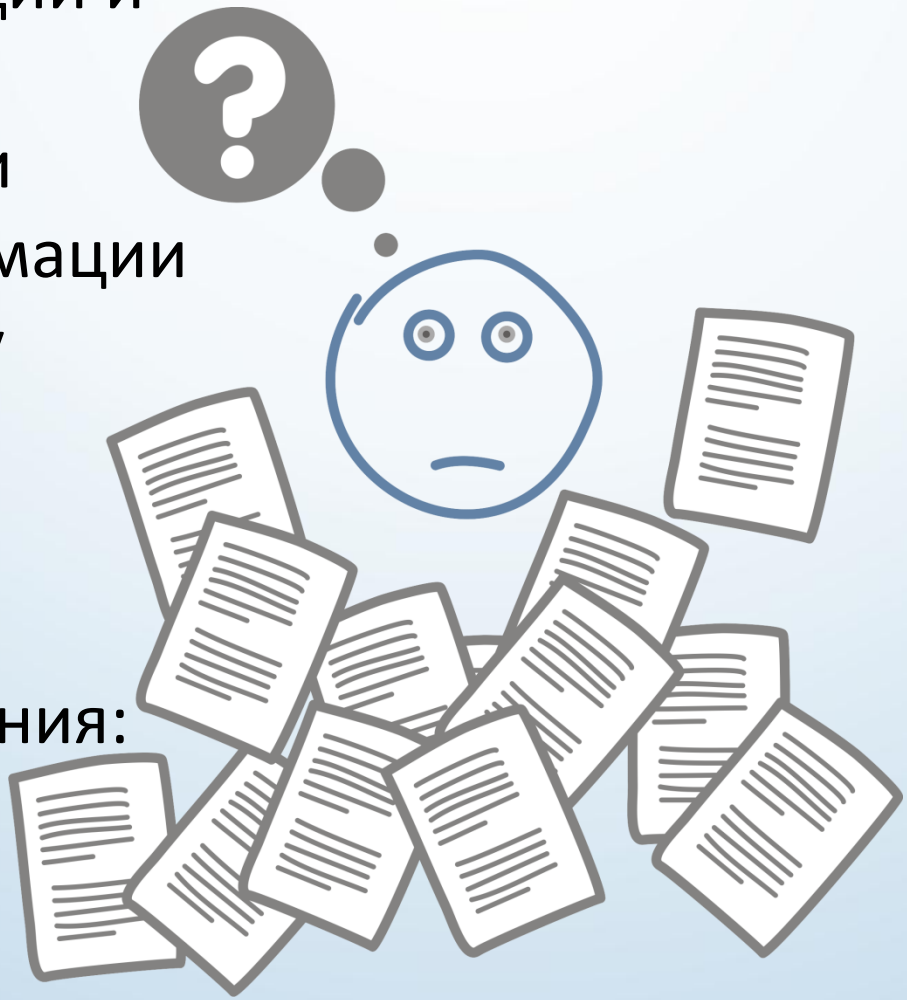
- Вместе с плотностью растут и ставки потерь
- Кроме мониторинга и аудита новых элементов архитектуры, необходимо также реализовать правила выявления специализированных инцидентов, присущих виртуальной среде



Миф 7. Аттестовать виртуальную инфраструктуру по требованиям российского законодательства – невозможно

Virtualization Security Group Russia
группа специалистов

- Методические рекомендации и материалы регуляторов по обеспечению безопасности конфиденциальной информации не делают различий между физической и виртуальной средой обработки
- Решения прошедшие сертификационные испытания:
  - Citrix XenApp 4.5
  - vGate for VMware VI



Virtualization Security Group Russia

группа специалистов

Вопросы?

maria.sidorova@virtualizationsecuritygroup.ru
http://www.virtualizationsecuritygroup.ru