Информационная безопасность (ИБ) и защита персональных данных в виртуальной инфраструктуре (ВИ)

Михаил Козлов

Консультант по развитию

http://devbusiness.ru/mkozloff

Михаил Козлов

Консультант по развитию бизнеса и продаже решений на основе бизнес-ценности (ROI)

20 лет в ИТ и консалтинге

VDEL, Trend Micro, VMware, Microsoft, V6, CARANA, Cognitive Technologies…

Сокращения

АИБ (АВИ) – администраторинформационной безопасности (виртуальной инфраструктуры)

ВИ/ВС – виртуальная инфраструктура/среда

ВМ – виртуальная машина (англ. VM)

ИБ – информационная безопасность

ИС – информационная система

НСД – несанкционированный доступ

ПДн – персональные данные

СВТ – средствавычислительной техники

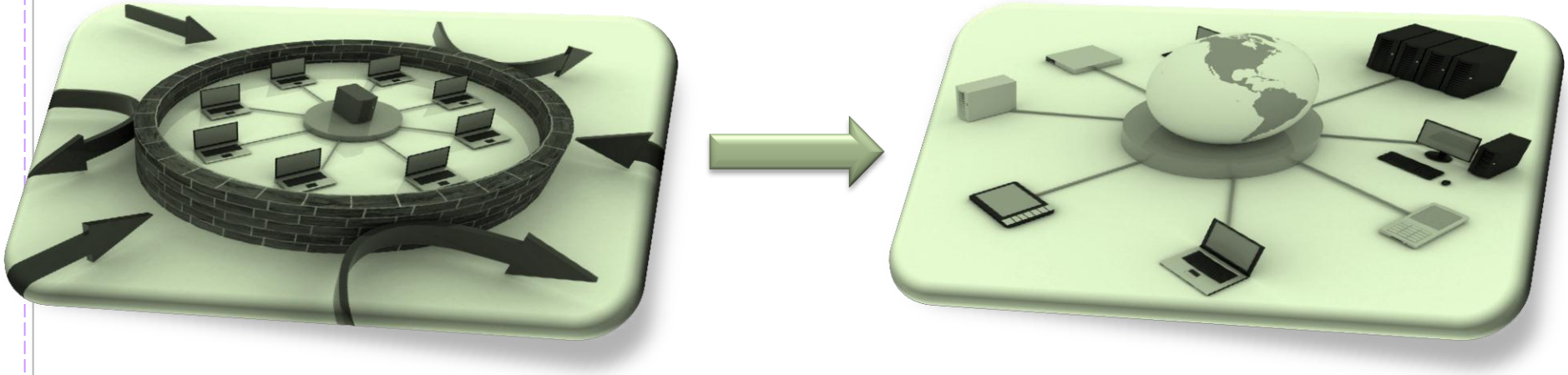
СЗИ – средство защиты информации

СХД – система хранения данных (Storage) или сеть хранения данных (SAN)

Содержание

Виртуализация и новые риски	• Ключевые риски • Кто контролирует администратора?
Виртуализация, облака и безопасность	• Лучшие практики по защите
Виртуализация и защита персональных данных	• Требования к ИСПДн • Сертификация платформы • Наложенные средства

Изменение парадигмы



Облачно с вероятностью осадков

"Тревога о безопасности сдерживает ИТ менеджеров от ухода в облака."

-The Economist, March 5, 2010

Виртуализация и риски ИБ

- **Специалисты ИБ не участвует в проекте по виртуализации**
- Взлом слоя виртуализации может привести к взлому всех ВМ
- Виртуальные ВМ-ВМ сети плохо контролируемы
- ВМ с разным уровнем ИБ размещены на одном физическом хосте
- Отсутствие контроля за действиями администратора
- Потеря разделения ответственности за сеть и ИБ

Источник:
Gartner, 2010

2010, безопасность и виртуализация

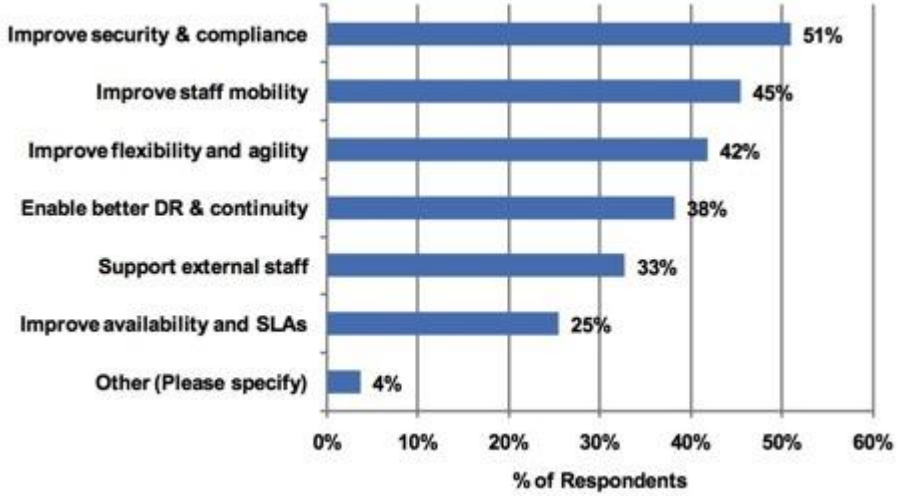
Появились новые изощренные виды монетизации киберугроз

Виртуализация инфраструктуры – ключевой тренд в корпоративных ИТ

- VDI
- Облака

Как обстоят дела с безопасностью виртуальных инфраструктур?

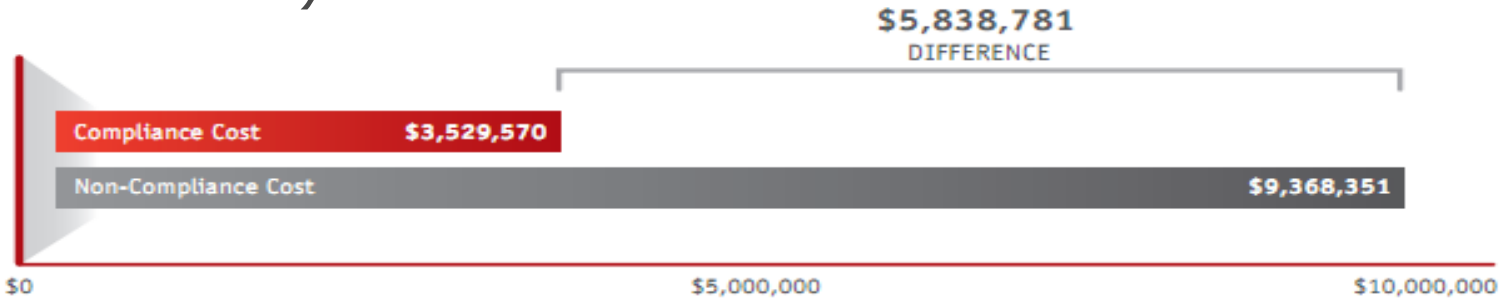
Приоритеты клиентской виртуализации 2011



Источник: http://www.enterprisemanagement.com/

Стоимость потери информации

- 285M взломанных записей в 2008 г. (Verizon Business RISK Team)
- В 2008 в США потеря каждой записи стоила $202, включая $152 косвенного ущерба (Ponemon Institute)



True Cost of Compliance Report, Ponemon Institute LLC, January 2011

Типы и стоимость инцидентов с ИБ

Type of Incident	Cost of incidents, last 2 years	Cost per incident
A rogue employee stole sensitive company documents (n=92)	$380,701	$362,572
An outside business partner lost a laptop containing sensitive information (n=77)	$320,137	$340,571
An outside attacker compromised a server and stole data (n=68)	$313,754	$295,994
An IT administrator abused privileges and stole data (n=73)	$312,044	$452,238
An outside business partner lost sensitive information via other means (n=88)	$303,268	$115,751
A supply chain or business partner abused their privileges and obtained data they should not have had access to (n=66)	$289,815	$362,269
IT operations lost an unencrypted backup tape or drive (n=84)	$277,481	$179,020
A terminated employee stole information because they had not been adequately de-provisioned (n=86)	$265,759	$160,096
A rogue employee used their privileges to access sensitive company documents that they had no business reason to view/use (n=109)	$246,641	$82,214
A customer service representative inappropriately accessed customer records (n=87)	$195,548	$54,929
An employee lost a laptop containing sensitive information (n=157)	$179,341	$26,335
An employee accidentally emailed or posted sensitive information (n=152)	$174,242	$25,586
An employee lost a smartphone (n=159)	$133,639	$11,826

Потеря данных через администратора – самый дорогой тип инцидента в ИБ

- В виртуальной среде нет проактивных средств контроля действий администратора
- Зловредное ПО с правами администратора может получить контроль над ВМ в обход гипервизора

An IT administrator abused privileges and stole data (n=73)	$312,044	$452,238

The Value Of Corporate Secrets
How Compliance And Collaboration Affect Enterprise Perceptions Of Risk
March 2010, Forrester

Что делать?

Разделить полномочия
и ответственность
администраторов
ВИ и ИБ

Лучшие практики информационной безопасности

БЕЗОПАСНАЯ ВИРТУАЛИЗАЦИЯ

Виртуализация и безопасность

Люди

- Обучение
- Разделение ответственности

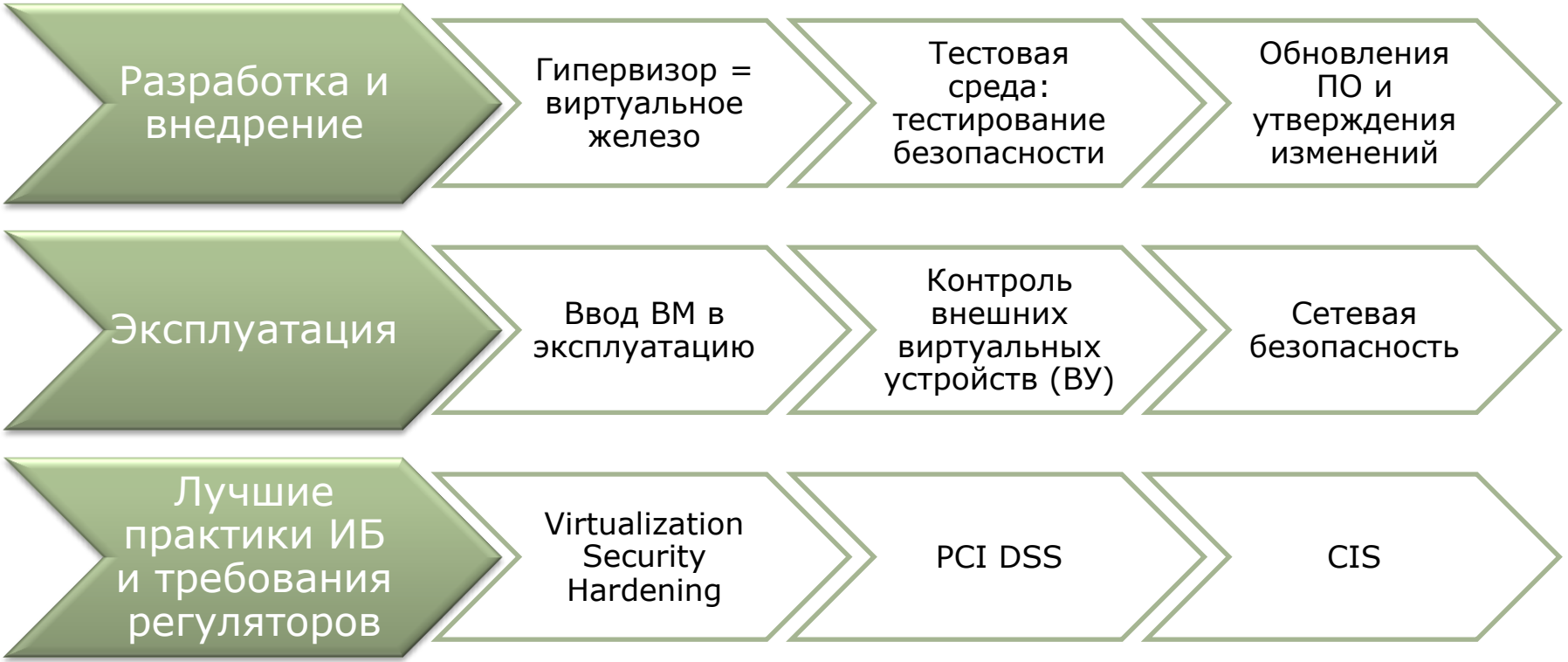
Процессы

- Лучшие практики
- Требования регуляторов

Технологии

- Платформа
- Наложенные средства

Ключевые процессы



Традиционные средства защиты в виртуальной среду не эффективны

- Firewall, VPN
- Антивирусы
- DLP
- IDS/IPS
- Другие средства защиты

М.б. неприменимы или снижать производительность среды

Нужны специальные средства

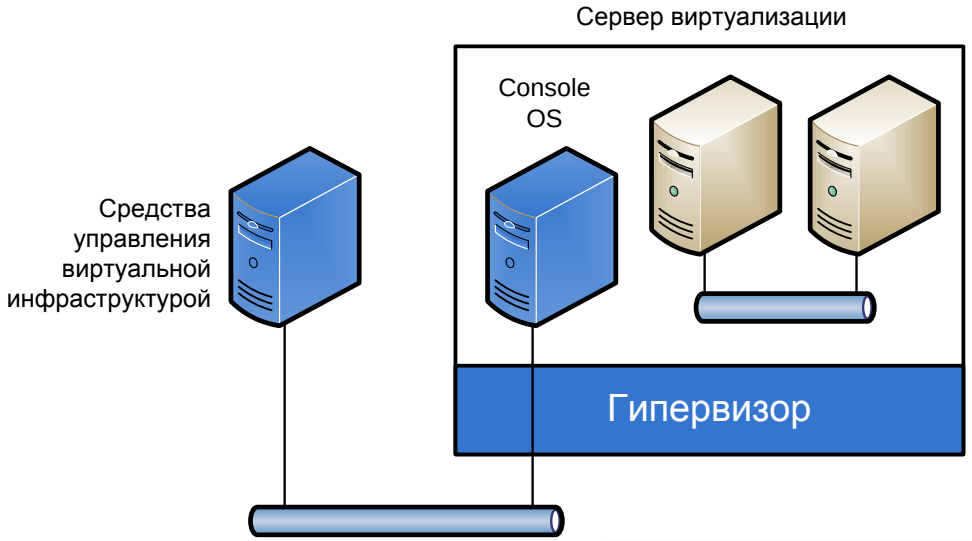
...

Безопасность гипервизора

Пока не обнародовано ни одного случая взлома гипервизоров или нарушения изоляции ВМ

Возможности Blue Pill & Red Pill пока не доказывают наличие угрозы для гипервизоров, **НО**

Можно получить доступ к гипервизору через средства управления

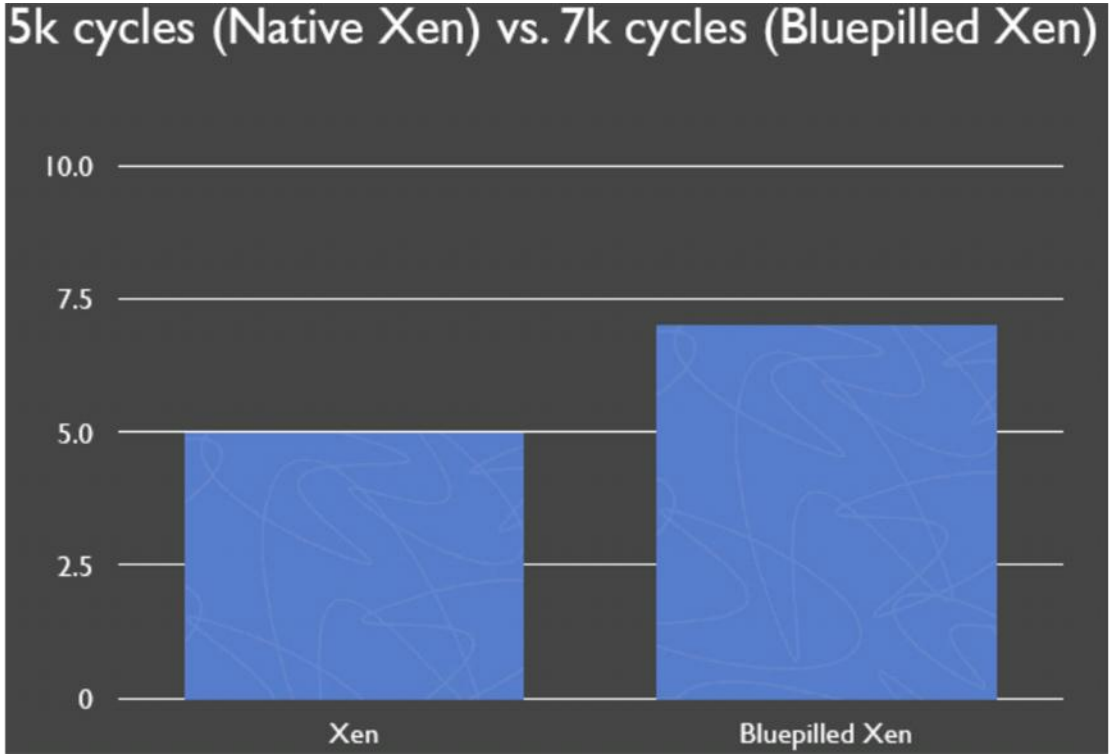


Матрица и безопасность виртуальной среды

Red Pill – способ обнаружения присутствия на физическом хосте работающей виртуальной машины

Blue Pill – зловредный гипервизор, незаметно превращающий ОС в ВМ и перехватывающий ее трафик

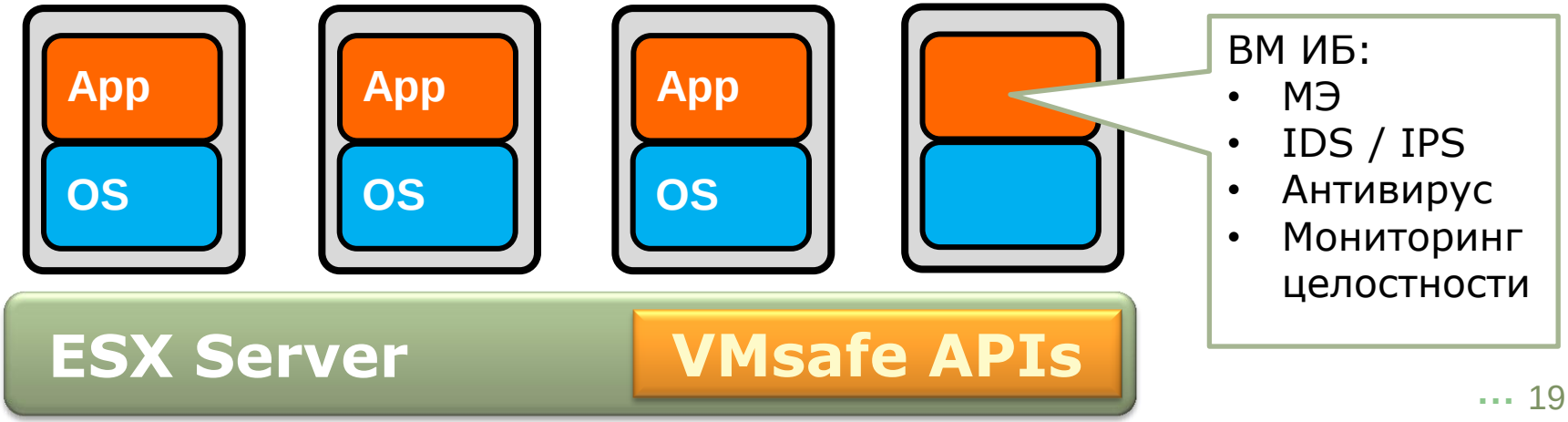
Обнаружить blue pill можно только по деградации производительности:



Ядро (kernel) гипервизора VMware

ESX – самое маленькое ядро на рынке

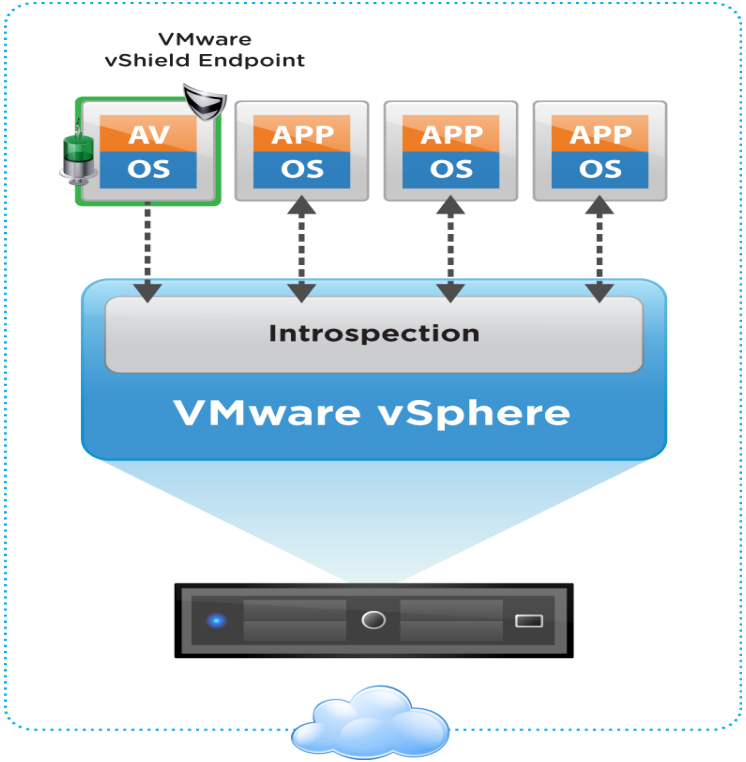
VMware VMsafe – API к ядру гипервизора: позволяет «видеть» идущий через него трафик (аналог для Hyper-V отсутствует)



Средства платформы: vShield Endpoint

Антивирусная зашита гостевых ВМ

Позволяет использовать специальную антивирусную ВМ без A/B агентов в гостевых ВМ



ОС в консоли управления

По слухам для vSphere 5 будет упразднена

Для VI 3 и vSphere 4 (Linux based)

- Подвержена обычным угрозам для ОС
- Используйте рекомендации «VMware Security Hardening Guide»
- Трудоемкая ручная настройка автоматизируется с vGate

VMware Linux Clients Advisory

- Трафик между клиентом vSphere и vCenter зашифрован (SSL+сертификаты)
- Linux клиенты, выполняющие vSphere клиента не проверяют годность сертификатов
- Угроза атаки man-in-the-middle
- Рекомендация VMware не использовать Linux клиент для управления

Файлы конфигурации ВМ

- Уделяйте отдельное внимание их защите и поддержанию целостности
- VMware .vmx файлы контролируют все параметры и настройки
- VMX файлы – это простой редактируемый текст
- Зловреды могут их читать и модифицировать

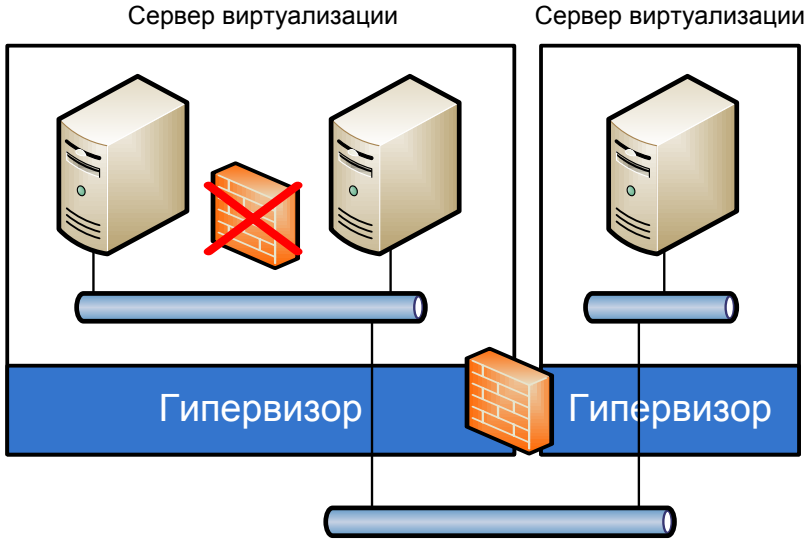
Виртуализация меняет свойства сетей

Стандартные МЭ становятся не везде применимы

Угроза DoS атаки: ВМ может занять весь трафик

- Мониторинг и ограничение ресурсов

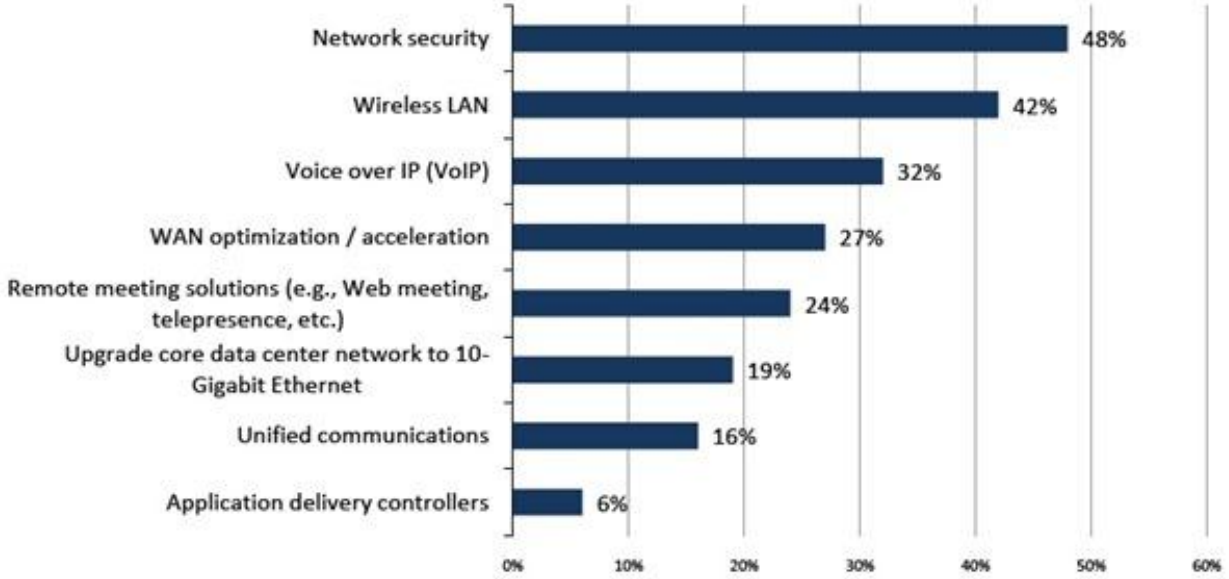
Трудоемкая ручная настройка параметров ИБ автоматизируется с vGate



Сетевая безопасность – приоритет №1

Figure 2. Top Areas for Networking Investments in 2010

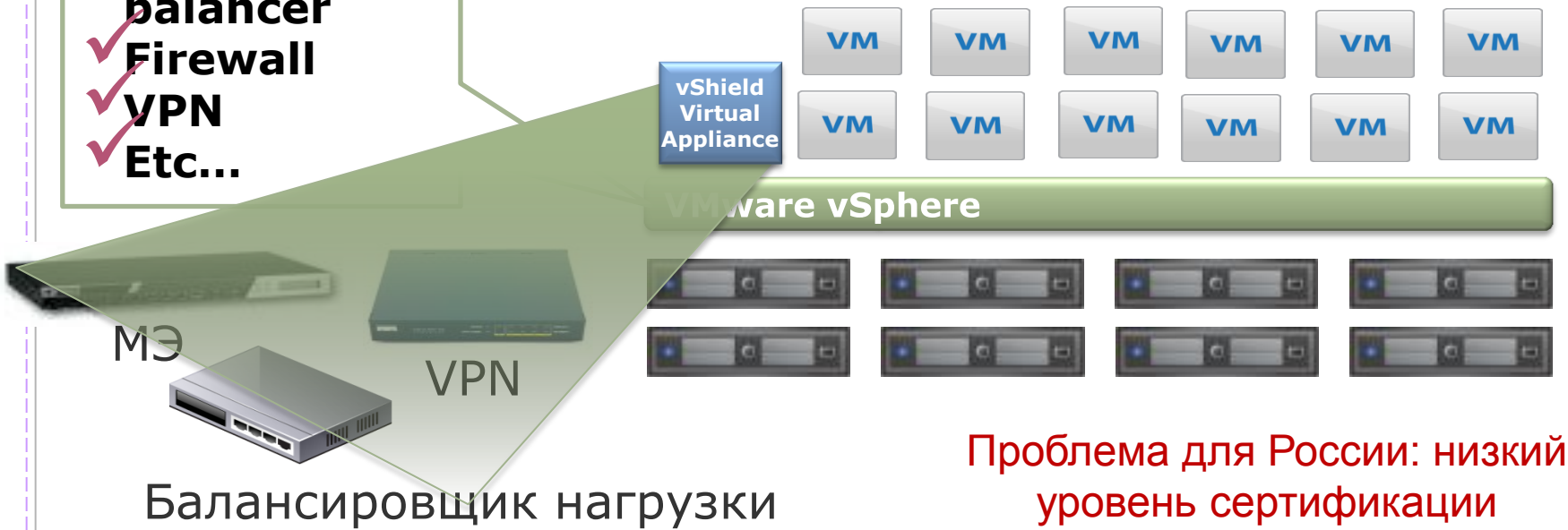
With regards to specific spending plans for networking, in which of the following areas will your organization make the most significant investments over the next 12-18 months? (Percent of respondents, N=264, up to three responses accepted)



Source: Enterprise Strategy Group, 2010.

VMware vShield: балансировка нагрузки, МЭ, VPN, зоны безопасности

- Load balancer
- Firewall
- VPN
- Etc…



Проблема для России: низкий уровень сертификации

Сетевой трафик для vMotion

Синхронизация памяти по Сети ХД без шифрования

Должна использоваться защищенная сеть, но:

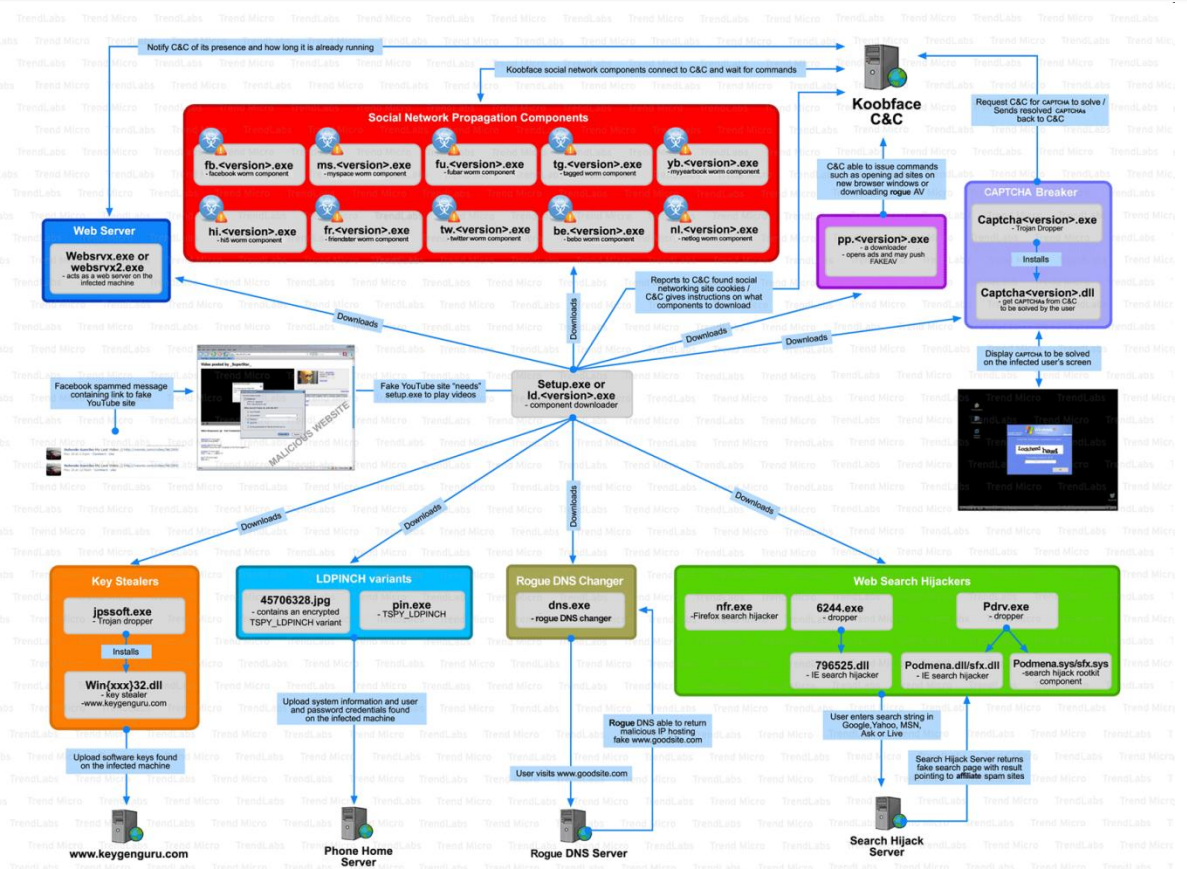
Любой ввод/вывод (LAN,RAM, HDD) чувствителен к угрозам типа **Man in The Middle**

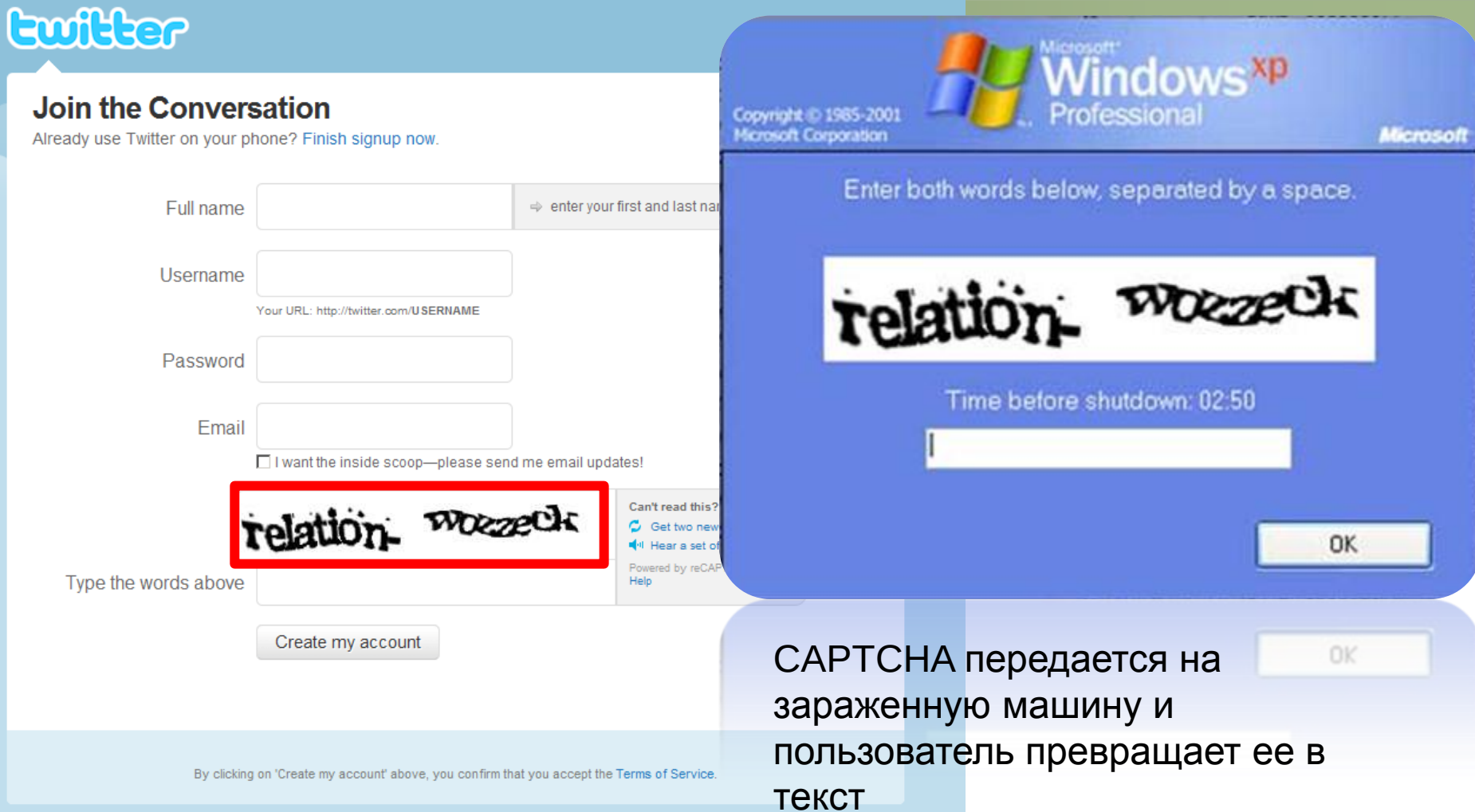
CAPTCHA [ˈkæptʃə] (от англ. «***C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part*» — полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей)

ПРИМЕР ОБХОДА CAPTCHA В СТИЛЕ MAN IN THE MIDDLE

Koobface

Пример сложного социального зловреда, использующего технику MitM





CAPTCHA передается на зараженную машину и пользователь превращает ее в текст

Защита от атак «Man in the Middle»

Перед вводом в эксплуатацию все самоподписанные SSL сертификаты необходимо заменить на доверенные сертификаты 3-х сторон

Гипервизор и спящие (выключенные) ВМ

Гипервизор может читать и изменять данные ВМ, когда они не работают

У проснувшейся ВМ устареют настройки безопасности

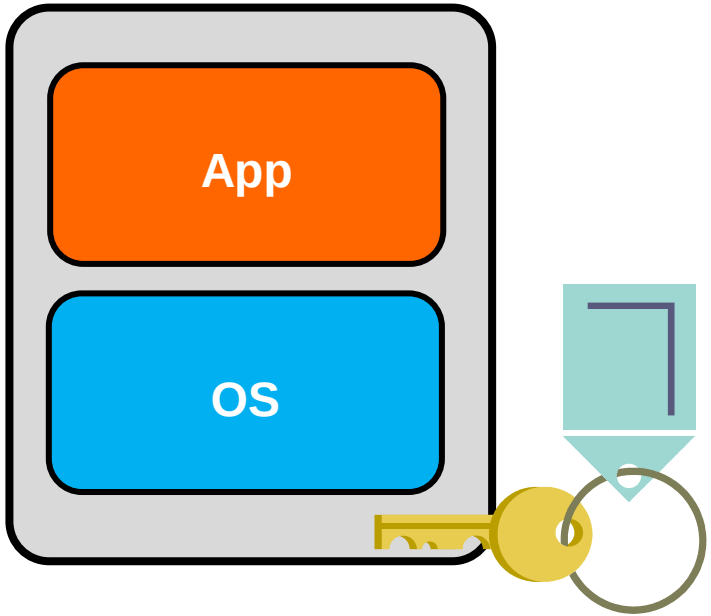
Аппаратные средства защиты в виртуальной среде

Могут не работать в ВС

- Традиционные средства доверенной загрузки.
- Во многих случаях аппаратное средство нельзя «пробросить» в виртуальную машину

Используйте стандартный образ ВМ с максимальными настройками ИБ

Заблокированный стандартный образ ВМ позволит избежать ошибок настройки ИБ



Изолированные (Out of Band) сети для управления виртуальной инфраструктурой

- Все управление ВИ должно осуществляться в изолированной OOB сети
- ВМ по умолчанию не должны иметь к ней доступ
- ВМ могут иметь доступ к OOB сети только через средства ИБ (МЭ, VPN, IPS, ...)
- Используйте технологии NAC или VPN для контроля ролевого доступа, аудита и шифрования трафика в/из сети управления

Сегментация системы хранения данных

- СХД гипервизора должна быть отделена от СХД, к которой имеют доступ ВМ (особенно для NFS)
- Разделение СХД между гипервизором и ВМ разрушает концепцию изоляции трафика
- Отделите трафик СХД (iSCSI, NFS…) от промышленного (production) трафика
- Включите двунаправленную аутентификацию CHAP для iSCSI
- Используйте SAN Zoning и LUN Masking

Лучшие практики ИБ для виртуальных сред

- PCI DSS 2.0
- CIS VMware ESX Server Benchmarks
- VMware Security Hardening Best Practices
- Hyper-V Security Guide

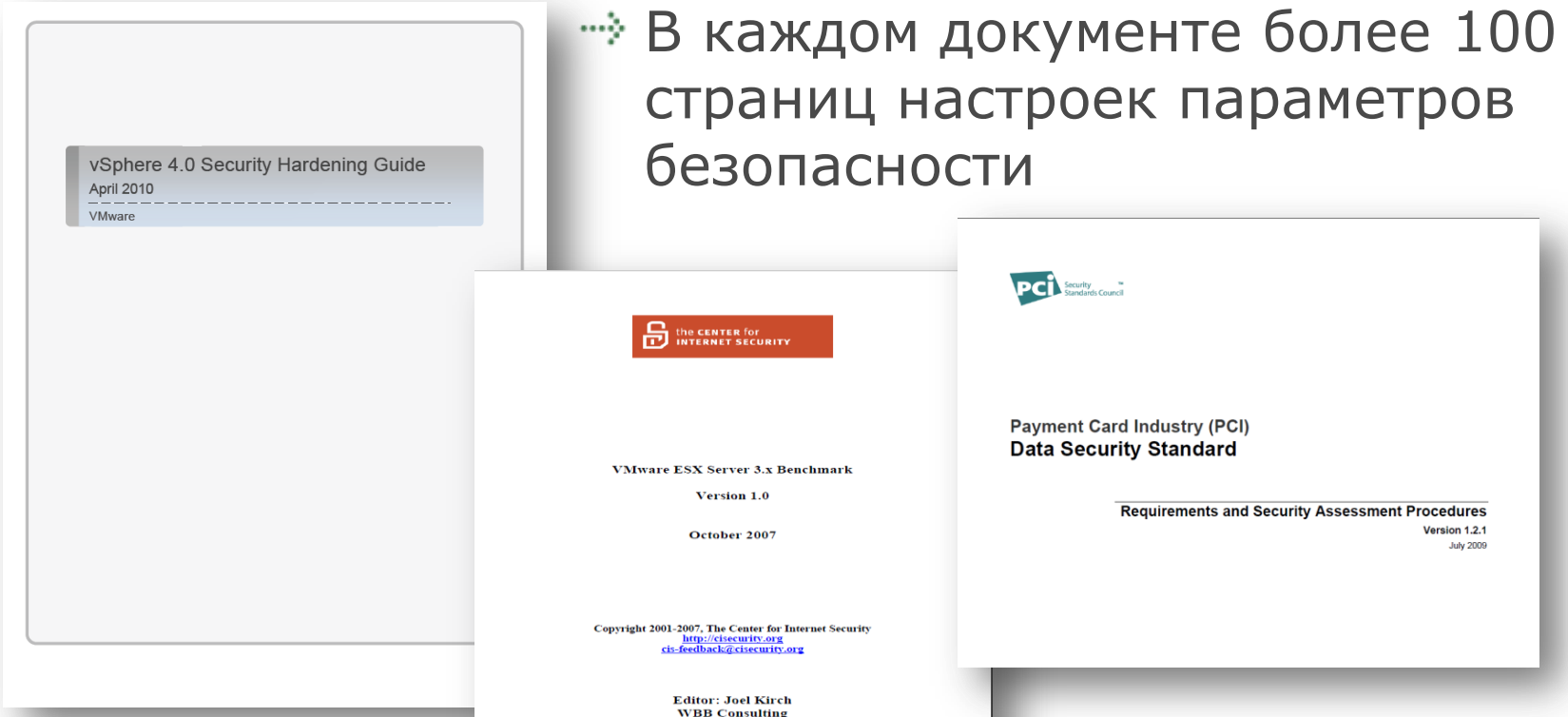
PCI Security Standards Council™

the CENTER for INTERNET SECURITY

vmware®

В каждом документе более 100 страниц настроек параметров безопасности

Лучшие практики ИБ для виртуальных сред



- В каждом документе более 100 страниц настроек параметров безопасности

Hypervisor Rootkit Detection

- HookSafe (Microsoft и NC State)
- Hypersight Rootkit Detector
- Intel Trusted Boot

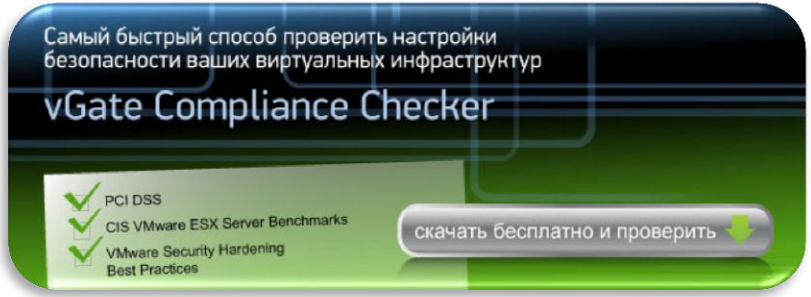
Применение лучших практик

Ручная настройка VMware или Hyper-V

- **или**

автоматизация с vGate for VMware: поставляется с шаблонами настройки для соответствия лучшим практикам ИБ

Как узнать правильность моих настроек?



Hyper-V Best Practices Analyzer for Windows Server 2008 R2

Безопасность для VMware

Требования	Продукты VMware	Продукты партнеров
Управление конфигурациями, мониторинг, аудит	VMware vCenter Server VMware vSphere Host Profiles VMware vCenter ConfigControl (future)	• EMC Ionix for Virtualization • NetIQ Secure Configuration Manager • Tripwire Enterprise for VMware • **vGate for VMware (Код Безопасности)**
Управление процессами	VMware vCenter Orchestrator VMware vCenter Lifecycle Manager	
Обновление выключенных ВМ	VMware Update Manager	• Shavlik NetChk Protect
Безопасность виртуальных сетей	VMware vShield Zones vNetwork Distributed Switch	• Cisco • Checkpoint • Reflex • Trend Micro • **vGate for VMware (Код Безопасности)**

Некоторые решения для VMware

FEATURESSUMMARY

Product, Version	URL, Price	Agents	VM versions	Functions	Notable Features
BeyondTrust PowerBroker v6.2	Beyondtrust.com $1,600/server	Yes	ESX/ESXi all v3. and v4.; Citrix Xen; Solaris and IBM	Compliance, access control	Root ESX password protection
Catbird vSecurity 3.5	Catbird.com $1,995/per socket	Yes	ESX/ESXi all v3.5 and v4.; Citrix Xen	Compliance, Firewall/IDS	Deep inspection rules
HyTrust Appliance v2.1.2	Hytrust.com $1,000/host	No	ESX/ESXi all v3.5 and v4.	Access control, compliance	Root ESX password protection
Reflex Systems v2.9	Reflexsystems.com $1,800/per socket	Yes	ESX only, all v3.5 and v4.	Access, Compliance, Firewall/IDS	Topo map, network zones, change tracking
Trend Micro Deep Security v7.5	Trendmicro.com $1,100/VM	Either	ESX/ESXi all v3.5 and v4; and VMsafe	Anti-virus , Firewall/ IDS, Compliance	Deep inspection rules, reports

http://www.networkworld.com/reviews/2011/030711-virtualization-security-test.html

Безопасность Microsoft Hyper-V R2

- Входит в Windows 2008 Server OS
- Нет API для мониторинга трафика в гипервизоре
- Нет API для сторонних средств ИБ (МЭ, IPS…)
- В гипервизоре нет методов для определения rootkits
- Одна выявленная уязвимость за 2 года на рынке
- Поддерживает защиту от подмены (спуфинг) MAC адресов в виртуальном коммутаторе
- Надежная технология обновлений
- Hyper-V security Guide

Инструменты

5nine Virtual Firewall 2.0 for Hyper-V

vmware

VMware vShield: Firewall, зоны безопасности балансировка нагрузки, API

TREND MICRO

Контроль ИБ трафика для VMware, требует vShield

Код безопасности
ГК «Информзащита»

Контроль настроек ИБ, целостности и прав доступа для VMware

...

Вывод:

Пока не существует одного полного ИБ решения для ВИ ☹

VMware vShield – базовые возможности ИБ

Ясное разделение ответствен-ности

Сетевой администратор

Администратор ИБ

Администратор ВИ

Политики

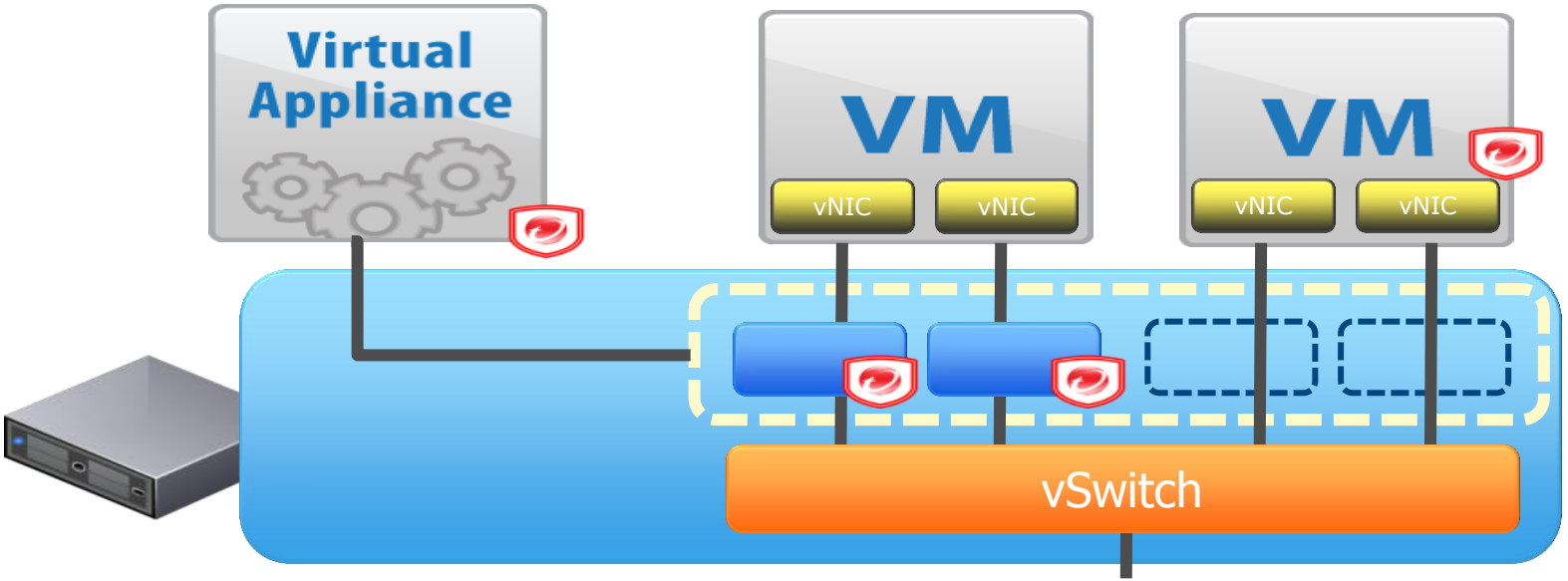
vShield Manager + vCenter

Простая настройка vShield

VM VM VM VM • • • VM VM VM VM

VMware vSphere

Trend Micro Deep Security for VMware

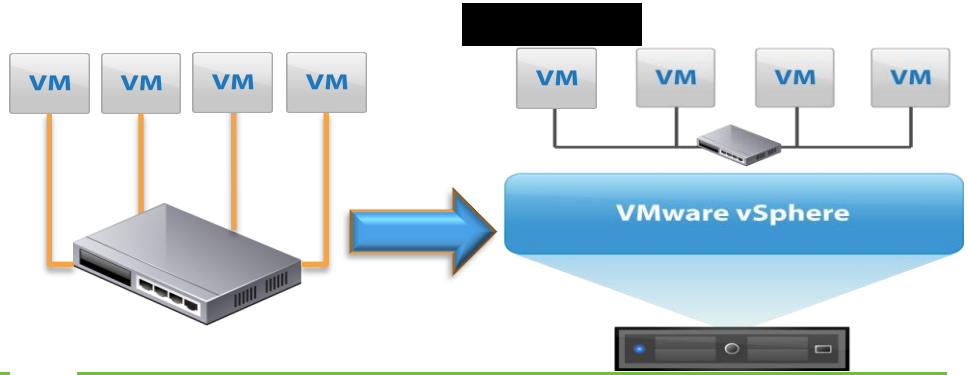


- Специальная гостевая виртуальная машина на гипервизоре
- Защищает все VM снаружи, без изменения VM
- FW, IDS/IPS и антивирусное сканирование на уровне гипервизора

Безопасность виртуальной инфраструктуры в облаках

ОБЛАКА И БЕЗОПАСНОСТЬ

Влияние виртуализации на ИБ ЦОД



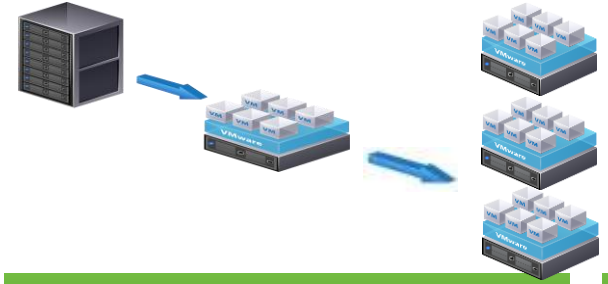
Абстракция и консолидация

- ↑ Экономия CapEx и OpEx
- ↓ Новый слой инфраструктуры
- ↓ Риски атак и ошибок конфигурации

Слияние коммутаторов и серверов

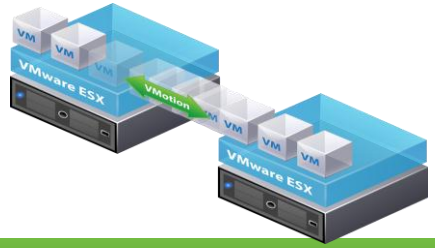
- ↑ Гибкость
- ↑ Экономия затрат
- ↓ Прозрачность сетевого трафика
- ↓ По умолчанию нет разделения ответственности

Влияние виртуализации на ИБ ЦОД



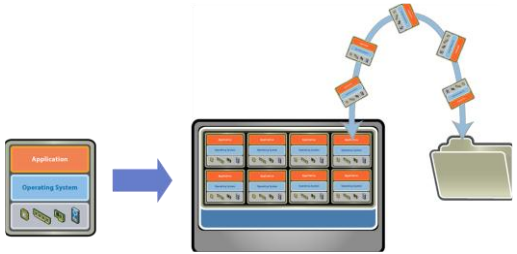
Быстрее внедрение

- ↑ Реакция ДИТ
- ↓ Тяжелее планировать
- ↓ Тяжело оценить текущее состояние
- ↓ Плохо описанные процессы
- ↓ Ошибки настройки



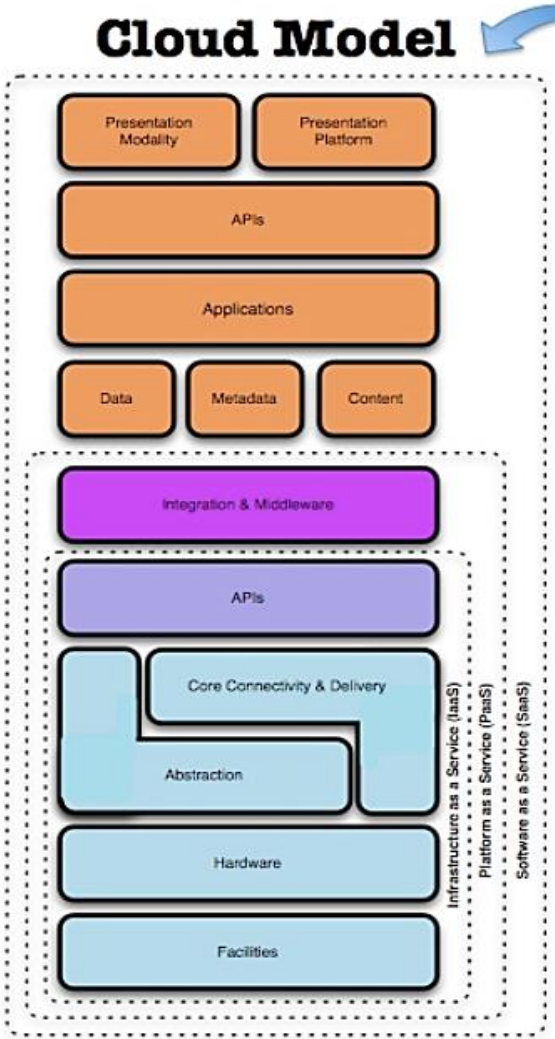
Мобильность ВМ

- ↑ Рост качества обслуживания
- ↓ ID не привязана к расположению



Инкапсуляция ВМ

- ↑ Проще внедрение и управление
- ↑ Не зависит от оборудования
- ↓ Устаревание настроек выключенных ВМ
- ↓ Выше риск кражи!



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

http://www.cloudsecurityalliance.org/

Консолидация = централизация рисков

- *«В облачной среде наименьший общий знаменатель безопасности будет разделен со всеми арендаторами виртуального ЦОД.»*

http://www.cloudsecurityalliance.org/csaguide.pdf

Ключевые угрозы в облаке v1.0

- Угроза #1: злоупотребление концепцией
- Угроза #2: небезопасные интерфейсы и APIs
- Угроза #3: вредоносные инсайдеры
- Угроза #4: общее использование старых технологий
- Угроза #5: утечки и потери данных
- Угроза #6: взлом учетных записей и сервисов
- Угроза #7: неизвестные характеристики рисков

Top Threats to Cloud Computing

Hardware Root of Trust

- Совместное предприятие Intel, RSA, RSA Archer Tech и VMware
- Проверка безопасности ВИ от чипов до гипервизоров

Intel TXT

- Trusted Execution Technology (TXT) - Intel TXT для защиты от атак на гипервизоры, BIOS и другой firmware
  - Разрешает миграцию ВМ только на доверенные хосты
  - При использовании совместно с Intel® Virtualization Technology (VT), дает возможность строить цепи доверенных отношений в ВИ

Trusted Platform Module (TPM)

- Элемент оборудования в основе цепи доверия для проверки загрузки
- Проверяет целостность ядра гипервизора и загружаемых модулей при старте с диска или из памяти

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

Регулирование и виртуализация

- PCI DSS
- 152ФЗ
- ЦБ РФ: СТО БР ИББС

Категории ПДн и классы ИСПДн

Категория ПДн	Описание категории ПДн	В зависимости от объема одновременно обрабатываемых ПДн		
		3	2	1
		менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации	от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн	более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом
4	Обезличенные и (или) общедоступные ПДн	К4	К4	К4
3	ПДн, позволяющие идентифицировать субъекта ПДн	К3	К3	К2
2	ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1	К3	К2	К1
1	ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	К1	К1	К1

Требования к наличию сертифицированных подсистем в СЗПДн

- Управление доступом
- Межсетевое экранирование
- Регистрация и учет
- Обеспечение целостности
- Антивирусная защита
- Обнаружение вторжений
- Анализа защищенности
- Шифрование

...

152ФЗ и VMware – как быть с ПДн? Ответственность с 1 июля 2011 г.

- VMware vSphere 4.1 в составе:
  - ESX 4.0 Update 1 и VMware vCenter Server 4.0 Update 1
- Сертификат ФСТЭК для использования в ИСПДн до К2 включительно

- vSphere 4.x + vGate
  - Сертификат ФСТЭК для использования в ИСПДн до К1 включительно

Сертификаты vGate for VMware Infrastructure

vGate 1.0 и 2

ФСТЭК СВТ 5 и НДВ 4

- для АС до 1Г включительно
- ИСПДн до К1 включительно

vGate 2 (в процессе)

ФСТЭК НДВ 2

- для АС до 1Б включительно
- ИСПДн до К1 включительно

Технологии ИБ vGate для ВС VMware

Управление конфигурациями

- Настройки ИБ гипервизора для защиты от НСД
- Контроль целостности

Управление доступом

- Защита от пользова-телей и админи-страторов

Защита данных на СХД и при передаче

СХД

- Шифрование и защита данных
- Защита от атак на файлы ВМ и сетевого трафика

ТМ, VMW

Аудиторский след

- Интеграция средств ВИ с SNMP или WMI уведо-млениями

Производительность

- Безопасность vs. Производи-тельность

ТМ, VMW

152ФЗ и Hyper-V– как быть с ПДн?

- Операционная система Microsoft Windows Server 2008 R2 в редакциях Standard, Enterprise и Datacenter
  - по 5 классу СВТ
    - 1Г
    - ИСПДн до 2 класса включительно
- Для К1 необходимы наложенные средства
  - Например, от Код Безопасности

http://www.fstec.ru/_doc/reestr_sszi/_reestr_sszi.xls

Сертифицированные наложенные средства защиты от «Код Безопасности» для использования Windows Server в ИСПДн К1

- TrustAccess:
  - Межсетевой экран
  - Регистрация и учет ПДн
  - Управление доступом
- SecretNet (ПО):
  - Мандатный доступ
  - Обеспечение целостности
- Соболь (АО):
  - Обеспечение целостности
- Security Studio Endpoint Protection
  - Антивирус
  - Обнаружение вторжений

Или бандл: Trust Access + Security Studio Suite

...

PCI-DSS: штрафы до $500,000

VISA

Personal Small Business **Merchants** Mid-Size & Large Companies Government

search go

New Acceptance Operations & Procedures **Risk Management** Marketing Center Payment Technologies Merchant Resources

Fraud Control Basics Online Safety **Cardholder Information Security Program** Verified by Visa Zero Liability Third Party Agent Program

IF COMPROMISED

Printable Page

- Overview
- Merchants
- Service Providers
- Payment Applications
- PIN Security
- **If Compromised**
- Training
- Alerts, Bulletins & Webinars
- Tools and FAQ
- Key Dates

If Compromised

Taking immediate action

Merchants and service providers that have experienced a suspected or confirmed security breach must take immediate action to help prevent additional damage and adhere to Visa CISP requirements.

Loss or theft of account information

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

If a member knows or suspects a security breach with a merchant or service provider, the member must take immediate action to investigate the incident and limit the exposure of cardholder data.

If a Visa member fails to immediately notify Visa Inc. Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information, the member will be subject to a penalty of $100,000 per incident.

Members are subject to fines, up to $500,000 per incident, for any merchant or service provider that is compromised and not compliant at the time of the incident.

On this page

- Steps for compromised entities
- Visa incident response team
- For more information

Top Downloads

What to Do If Compromised PDF | 821 KB

Responding to a Data Breach PDF | 352k

Qualified Incident Response Assessor List PDF | 32k

View all data security downloads

Соответствие требованиям PCI DSS 2.0

vSphere

- В ручную
- vGate for VMware

Hyper-V

- В ручную

PCI DSS 2.0: требования к виртуальной среде

- BM рассматривается как физический сервер
- Одна ключевая функция на BM
- Запрещено давать сотрудникам доступ к гипервизору
- Минимально необходимый уровень прав доступа
  - Например администратор BM не может назначить ей другой vSwitch
- Разделение функций и сетей с разными уровнями безопасности
  - На vSwitch нельзя использовать VLANs с 802.1Q, если у них разные функции или уровни безопасности (п. 2.2.1). Добавьте vSwitch для изоляции трафика
- Нельзя совмещать тестовые и производственные среды

vGate и PCI DSS

vGate поставляется с шаблонами настройки VMware для соответствия PCI DSS

www.sanctummovie.com

В безопасности не бывает мелочей

Дополнительная информация

- Подробнее о vGate:
  - http://www.securitycode.ru/products/sn_vmware/
- vGate Compliance Checker for VMware (free)
  - http://www.securitycode.ru/products/sn_vmware/vgtate_checker/
- Hyper-V Security Guide
  - http://bit.ly/dsrnXc
- Security Best Practices for Hyper-V and Server Virtualization
  - http://bit.ly/hq6chE
- Virtualization Security Overview by Cisco
  - http://isaca-ut.org/documents/speakers/2010/Virtualization Security Overview.pptx

Персональные данные в виртуальной инфраструктуре

Ситуация

Для ИСПДн К1 необходимо использовать сертифицированные ФСТЭК средства, включая НДВ

Виртуализация несет новые риски ИБ

Последствия

vSphere и HyperV в России не могут использоваться в ИСПДн К1

В виртуальной среде можно украсть весь бизнес

Решение

Включить специалистов ИБ в проекты виртуализации

Использовать наложенные средства ИБ

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?