

Тенденции рынка информационной безопасности

Владимир Мамыкин

к.э.н., MBA

Директор по информационной безопасности

ООО «Майкрософт Рус»

блог: <http://blogs.technet.com/mamykin/>

IT-Summit
3-4 апреля 2008 1

Источники роста экономики

■ Безопасность

- Так как для роста экономики необходимо увеличение использования электронных платежных систем, электронных идентификаторов личности и электронных документов – а их использование зависит от доверия к ним пользователей, которое основывается на безопасности этих систем

■ Общие стандарты

- 37% опрошенных руководителей считают отсутствие стандартов главной внешней проблемой, так как единые стандарты устраняют риск инвестиций в конкурирующие технологии

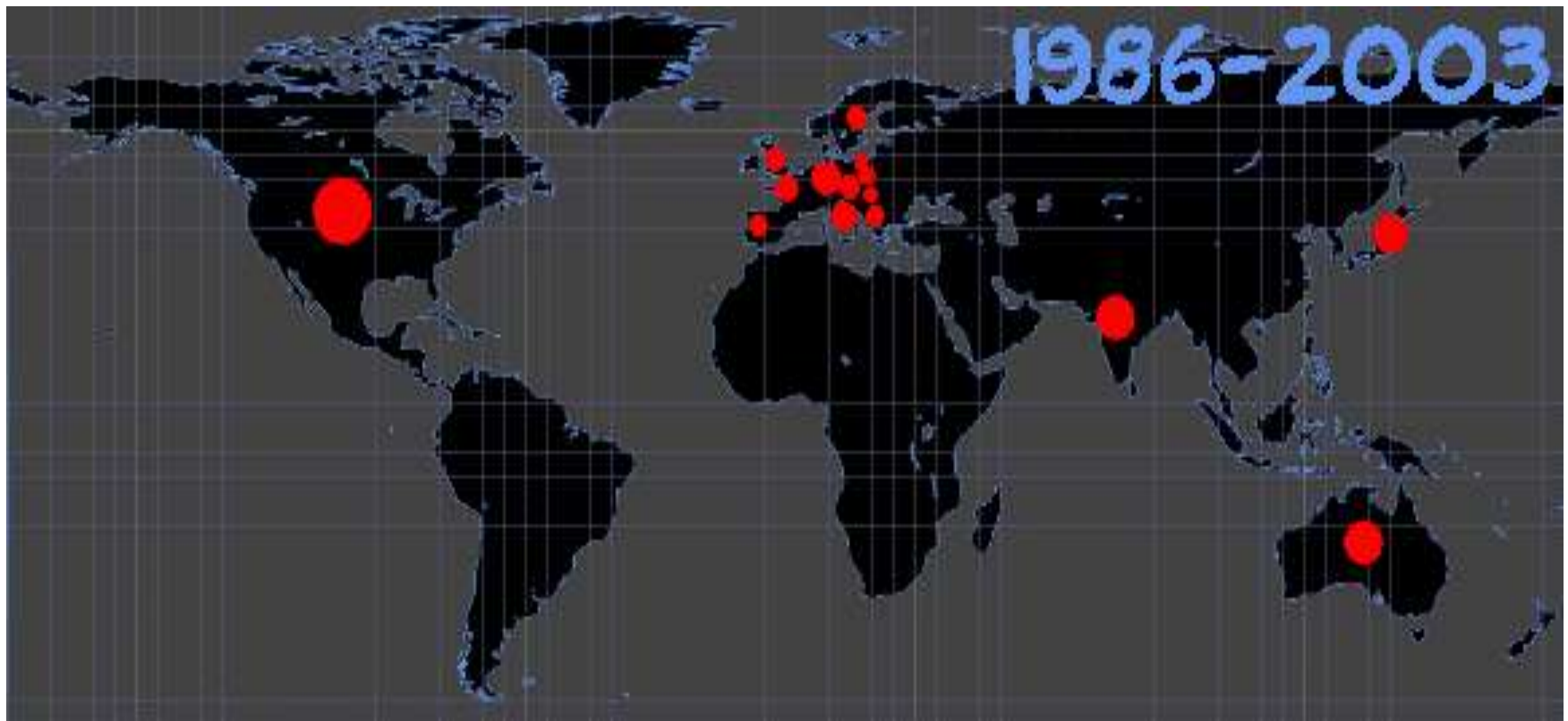
■ Интеллектуальная собственность

- Основная роль в создании инновационной культуры в стране, в защите инвестиций, в росте инвестиционной привлекательности страны

Источник: Отчет «Reaping the benefits of ICT: Europe's productivity Challenge», аналитическая служба «The Economist» www.eiu.com

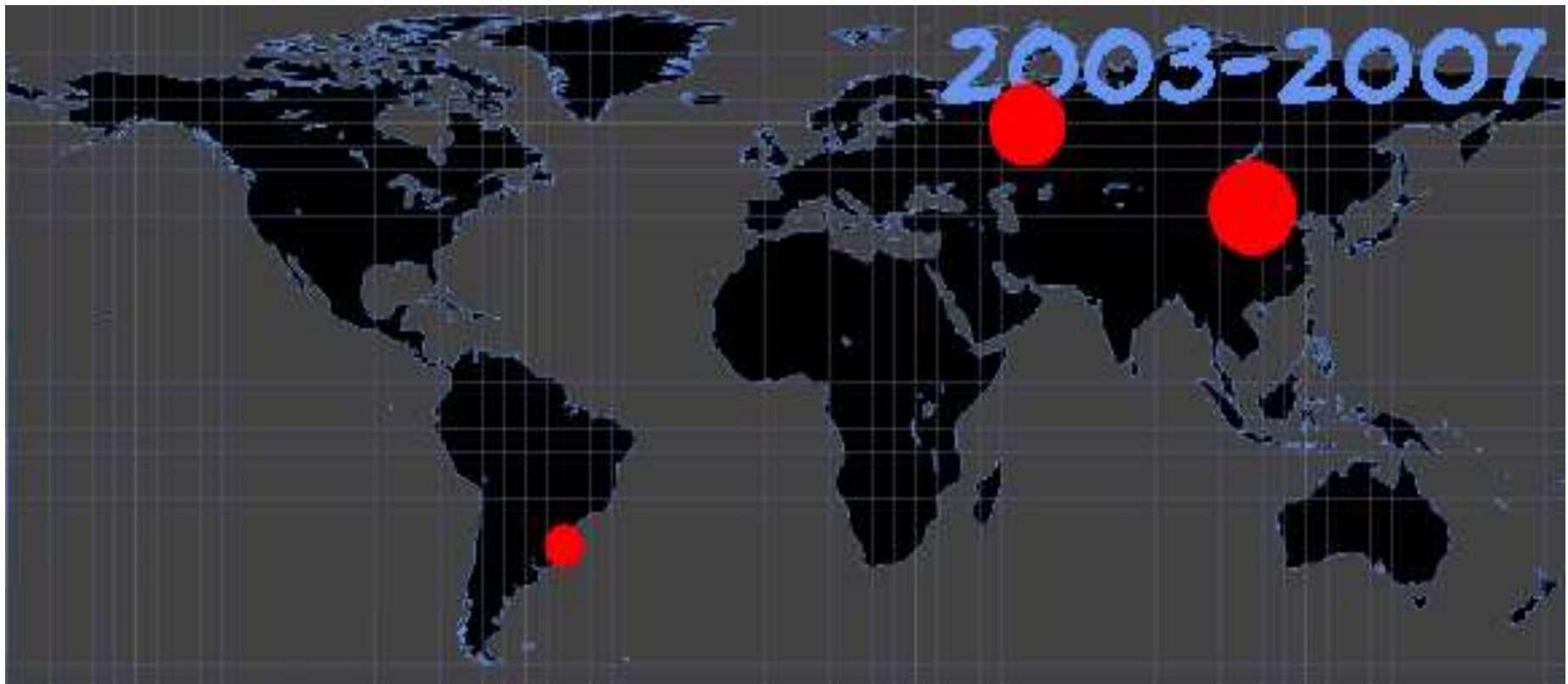
История вирусописателей - 1

Старая школа из США, Европы и Японии
Вирусописание как хобби



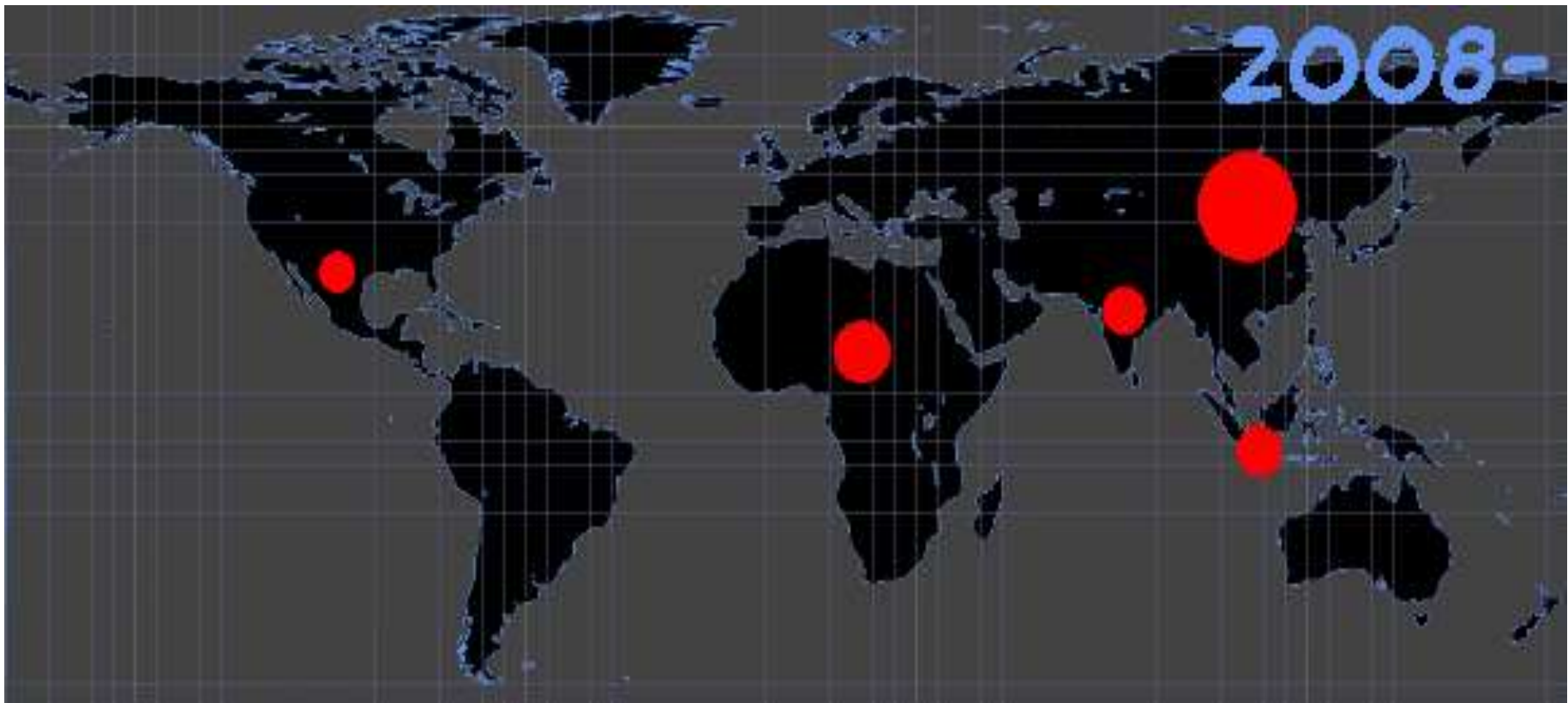
История вирусописателей - 2

Сегодняшняя школа из Китая, России и Южной Америки
«Профессионалы-налетчики»



История вирусописателей - 3

Новые школы из Центральной Америки, Африки и Юго-Восточной Азии
Причины: развитие Интернета, отсутствие работы в ИТ секторе,
слабое законодательство



Актуальность проблемы обеспечения безопасности

- Ущерб от вирусных атак по всему миру (*Computer Economics, 2007*)
 - 2006 - 13,3 млрд. долл.
 - 2005 - 14,2 млрд. долл.
 - 2004 - 17,5 млрд. долл.
- Общие убытки от нарушений безопасности
 - Ущерб на 1 сотрудника = 50 долл. в год
- Типы атак (2007 г., 436 компаний опрошено)
 - 59% компаний подвергались атакам со стороны своих сотрудников
 - 52% компаний подвергались вирусным атакам
 - 50% компаний фиксировали кражу ноутбуков и мобильных устройств

Некоторые тренды

Год	2007	2006	2005	2004
Число опрошенных компаний	194	313	639	269
Убытки на компанию (\$ тыс.)	345	166	203	526
Убытки от (\$ млн.):	2007	2006	2005	2003
Вирусные атаки	8	16	42	27
Неавторизованный доступ	1	11	31	0,5
Отказ в обслуживании	3	3	7	65
Финансовое мошенничество	21	-	-	-
Кража ноутбуков	4	7	4	7

Источник: 2007 CSI Computer Crime and Security Survey

Расходы на ИБ

На 1 сотрудника в год

Оборот компании	На операционные расходы	На капитальные вложения	На тренинги	Суммарные расходы
Более 1 млрд. долл.	142	58	18	198
Более 100 млн.долл.	92	34	22	126
Более 10 млн.долл.	241	220	111	461
Менее 10 млн.долл.	602	746	318	1349

Источник: 2006 CSI/FBI Computer Crime and Security Survey

Некоторые выводы из отчета CSI

- Максимальные финансовые потери – от финансового мошенничества
- Самые популярные средства
 - Антивирусные средства - 98% (было 97%)
 - Межсетевые экраны – 97% (было 98%)
 - Виртуальные частные сети (новая номинация) – 84%
 - Антишпионские средства – 80% (было 79%)
- Не смотря на разговоры об аутсорсинге ИБ – почти никто не пользуется
- Большинство компаний (84%) используют ROI и другие инструменты для оценки инвестиций в ИБ (ранее – 60%)
- В среднем 5% ИТ бюджета идет на ИБ
 - В России – 0,5% ИТ бюджета идет на ИБ

Уязвимости за 2007 + 1 кв. 2008

в скобках – за все время существования продукта

■ Linux Kernel 2.6	32 + 4 (всего 143)
■ Red Hat Enterprise Linux Server v.5 *)	97 + 21 (всего 118) + ядро
■ Sun Solaris 10	88 + 22 (всего 194)
■ Microsoft Windows Server 2003 Ent.	31 + 5 (всего 150)
■ Apple Mac OS X –	26 + 3 (всего 116)
■ Red Hat Enterprise Linux Client v.5 *)	99 + 23 (всего 122) + ядро
■ Windows XP Professional	30 + 5 (всего 203)
■ Windows Vista	17 + 5 (всего 25)
■ Oracle Database 10.x	6 + 1 (всего 20)
■ IBM DB2 Universal Database 8.x	5 + 1 (всего 19)
■ MySQL 5.x	6 + 1 (всего 12)
■ Microsoft SQL Server 2005	0 + 0 (всего 0)
■ Cisco Pix 6	1 + 0 (всего 12)
■ Microsoft ISA Server 2006	0 + 0 (всего 0)

*) продукт 2007 года

ВЫЗОВЫ

Угрозы стали более опасны

- Более изощренные атаки
- Мотивированные получением прибыли
- Более частые
- Атаки движутся в направлении приложений

Фрагментарность технологий безопасности

- Очень много продуктов, которые не взаимодействуют
- Различные консоли управления для каждого продукта
- Невзаимодействующие продукты не позволяют проводить обобщенный анализ событий

Сложность использования, развертывания и управления

- Сложность выбора продукта и управления им
- Недостатки интеграции ведут к запутанности управления
- Цена установки и запутанность управления противодействуют всеобъемлющему развертыванию во всей сети предприятия

Ответ на вызовы: пути реализации безопасной среды

■ Доверенная экосистема

- Сквозная аутентификация в гетерогенных средах
 - Например, концепция Identity Metasystem

■ Инжиниринг технологий безопасности

- Повышение качества инжиниринга технологий безопасности на всех стадиях разработки
 - Например, Security Development Lifecycle в Microsoft

■ Упрощение и интеграция систем безопасности

- Например, интеграция систем безопасности и антивирусных средств с платформой в Windows Security Center в Windows XP SP2 и Windows Vista

■ Создание фундаментально безопасных платформ со встроенными

- технологиями изоляции процессов для снижения уровня воздействия вредоносного ПО
- технологиями доверенной многофакторной аутентификации
- средствами интеграции Политик контроля доступа и Политик безопасности
- унифицированными аудитами приложений

Некоторые итоги

- ❑ Основная тенденция – консолидация продуктов ИБ и их производителей вокруг крупных игроков (в алфавитном порядке): EMC, IBM, Microsoft, Oracle и других
 - ❑ Цели приобретений – создание простых в управлении интегрированных систем обеспечения безопасности
- ❑ У крупных игроков, ранее не очень известных на рынке ИБ, есть значительные достижения. Часто НЕ за счет приобретения известных компаний
 - ❑ Выпуск продуктов без уязвимостей (например, SQL Server 2005 и ISA Server 2006 от Microsoft)
 - ❑ Выпуск качественных «своих» продуктов ИБ (например, антивирус Forefront от Microsoft несколько раз обнаружил все 100% вирусов в престижных тестах VirusBulletin100)
- ❑ Продолжится рост числа новых компаний в сфере ИБ
 - ❑ как следствие роста числа новых угроз и необходимости поиска методов защиты

Новый тренд – аппаратно-программная защита информации на базе чипов

- Международным консорциумом Trusted Computing Groups (<http://www.trustedcomputinggroup.org>) разработаны стандарты чипов Trusted Platform Modules (TPM)
 - чип TPM предназначается для хранения паролей, криптографических ключей и цифровых сертификатов
 - TPM используется для контроля начальной загрузки компьютера, для предотвращения потери информации вследствие кражи компьютера
- Компьютеры с чипом TPM на материнской плате уже выпускаются в значительных количествах всеми производителями компьютеров
- TPM поддерживается множеством производителей: AMD, Intel, IBM, HP, Microsoft (на уровне операционной системы в Windows Vista)



СПАСИБО!!!

Владимир Мамыкин

блог: <http://blogs.technet.com/mamykin/>