

Методология построения и эксплуатации системы антивирусной безопасности крупного предприятия

Тимур Сабитов
Поликом Про
MCSE, МСТ, TCSM

Что такое информационная безопасность



■ Определение

- «Безопасность — желаемый уровень целостности, исключительности, доступности и эффективности для защиты данных от потерь, искажения, разрушения и несанкционированного использования», - *Б. Гейтс*

■ Почему акцент на антивирусную безопасность?

Основные угрозы

- Физическая защита (4%)
- Сбои в работе системы (20%)
- Электронные средства стороннего воздействия (20%)
- Нарушение конфиденциальности (25%)
- Вредоносный код (26%)
- Другое (5%)

Источник: «Обзор информационной безопасности отрасли в 2000 году», опубликованный Международной ассоциацией компьютерной безопасности (ICSA)

Вирусная угроза вчера

Название	Ущерб (\$ млрд.)	Cyber Quake Rating
■ Nimda	0.53	0.61
■ Code Red(s)	2.62	2.99
■ SirCam	1.05	1.20
■ Love Bug	8.75	10.00
■ Melissa	1.10	1.26
■ Explorer	1.02	1.17

Вирусная угроза вчера

	Название	Ущерб (\$ млрд.)
1	MyDoom	39
2	Sobig	37,1
3	Klez	19,8
4	Mimail	11,5
5	Yaha	11,5
6	Swen	10,4
7	Love Bug	8,8
8	BugBear	3,9
9	Dumaru	3,8
10	SirCam	3,0

* — по данным на 02.02.2004 г.

Эволюция критериев выбора

■ Давно

- Лучшее решение – 2 антивируса
 - Российский – «местные» вирусы
 - Западный – «залетные» 😊

■ Недавно

- Кто быстрее обновляет базы и лечит, тот и лучше

■ Сейчас

- Computer Antivirus Research Organization (CARO)
- Другие критерии выбора

Парадокс

- 96% предприятий имеют АВ-защиту
 - 43% страдают от вирусных атак !

- Плохие продукты?
 - Нет!

- Аналогия со строительством дома

Важно кто строит!



Традиционный подход

- Антивирусные системы предприятий - исторический результат «естественного роста»
 - Поэтапное развитие предприятия
 - Поэтапное развитие технологий
 - Поэтапное финансирование
- Следствия
 - Разнородность (многовендорные системы)
 - Отсутствие централизованного управления
 - Сложность обновления и модификации
- Снижение эффективности и увеличение ТСО

Методология построения

- Эволюция методов. Наш опыт

1. Защита всех точек проникновения

- Рабочая станция
- Файловый сервер
- Почтовая система
- Шлюз Интернет

Методология построения

■ Эволюция методов. Продолжение...

2. Централизованное управление

3. Поиск и устранение уязвимостей



Методология построения

■ Эволюция методов. Продолжение...

4. Упреждающие меры

- Предотвратить проникновение
- Ещё не лечить!!!

5. Автоматизация восстановления систем

- Предотвратить рецидив
- Удалить “грязь”
- Оценить ущерб

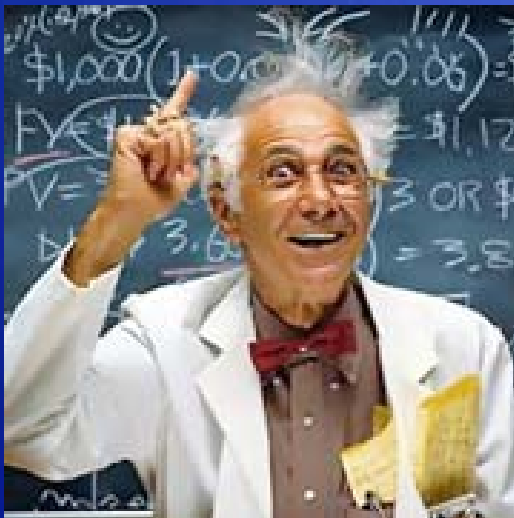


Методология построения

■ Эволюция методов. Продолжение...

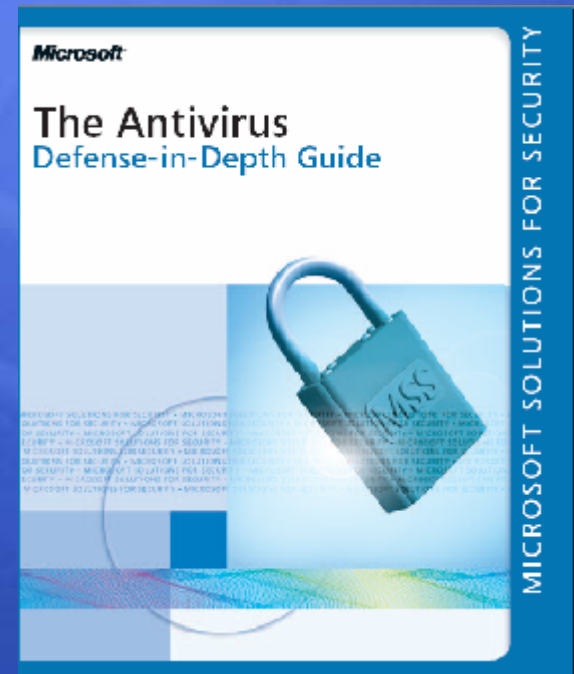
6. Защита на сетевом уровне

7. Обучение персонала



Antivirus Defense in Depth

- Методология из серии Microsoft Solutions for Security
- http://www.microsoft.com/technet/security/guidance/avdind_0.mspx



Модель Defense in Depth



Сложности внедрения

- Внедрение корпоративной системы качественно отличается от установки AV на 1 машину
- Требуются знания и опыт в области
 - Различных ОС, почтовых систем; МСЭ; прикладного ПО
 - Сетевых технологий от физического до прикладного уровня
 - Самих антивирусов (особенности, возможности...)
 - Продуктовых линеек и лицензионных схем
- Задача внедрения «однократна»
- Многие компании используют не своих специалистов, а обращаются к тем, кто много лет профессионально решает эти задачи!

Эксплуатация AV систем

■ Мониторинг

- Инциденты
- Обновление
- Апгрейд версий

■ Миграция

- Сложности удаления/замены ПО
- Мы умеем!!!

Почему мы рассказываем об этом

■ Наш опыт

- Центр Компьютерной Безопасности - 1999 г.

■ Крупные проекты в текущем году

Машиностроение	4
Металлургия	4
Нефтяная и нефтегазовая пром-ть	3
Пищевая промышленность	5
Транспорт	2
Угольная промышленность	1

Почему мы рассказываем об этом

- Наши компетенции. Партнёрство
 - Microsoft
 - Trend Micro
 - Veritas
 - Другие... 😊



Спасибо !

Контакты

Санкт-Петербург

(812) 325-84-00

Москва

(095) 730-96-71

(095) 956-99-75

info@polikom.ru