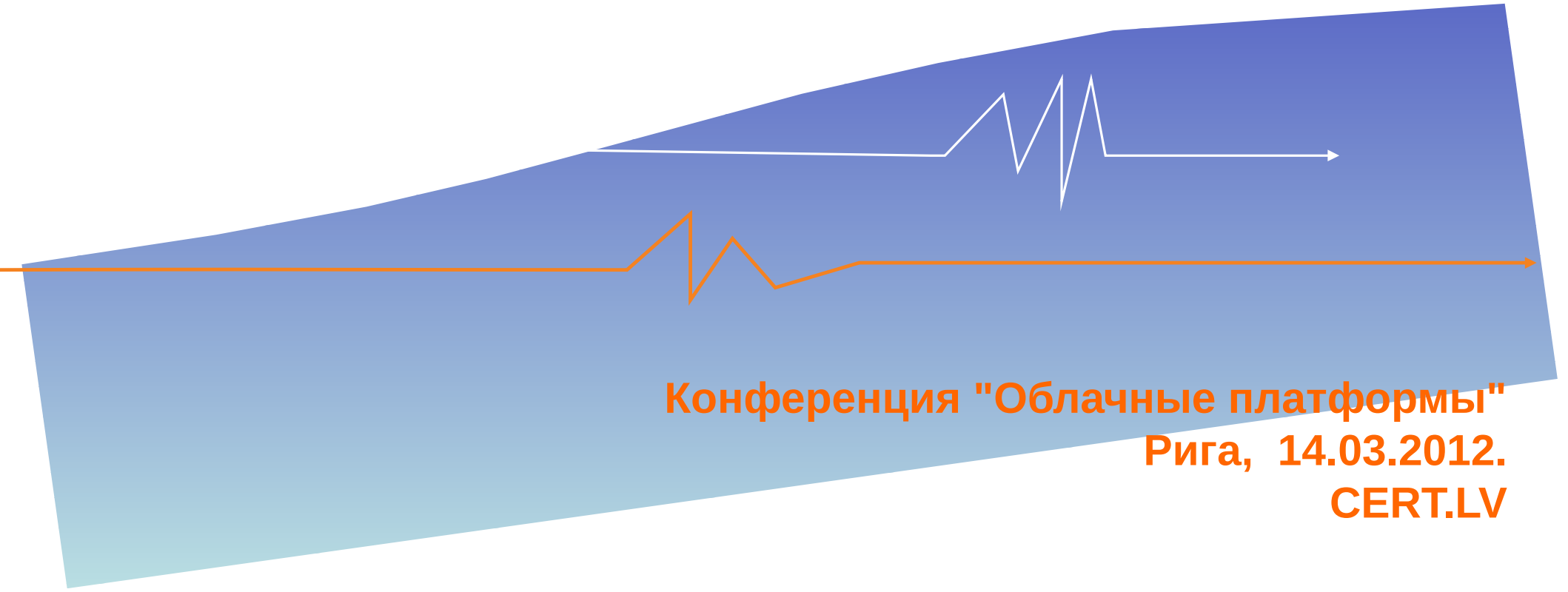
“Виртуальная атака - реальная угроза и потери!”



Конференция "Облачные платформы"
Рига, 14.03.2012.
CERT.LV

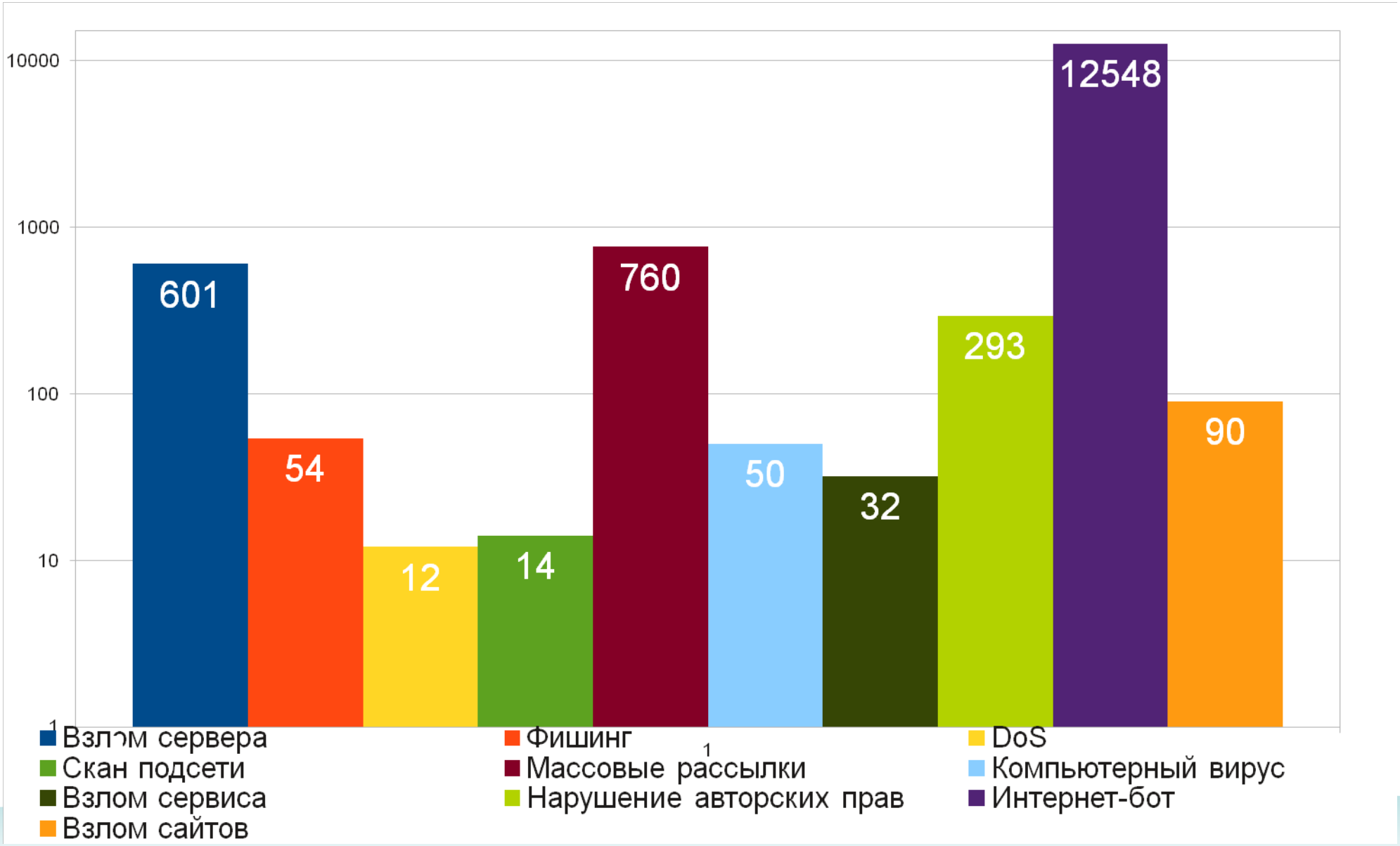
Содержание

- Введение, коротко о CERT.LV
- Статистика инцидентов
- Атаки на "облачные" сервиса
- Безопасность данных в "облаке"
- Интернет подключение - уязвимая точка предприятия
- Заключение

Введение, коротко о CERT.LV

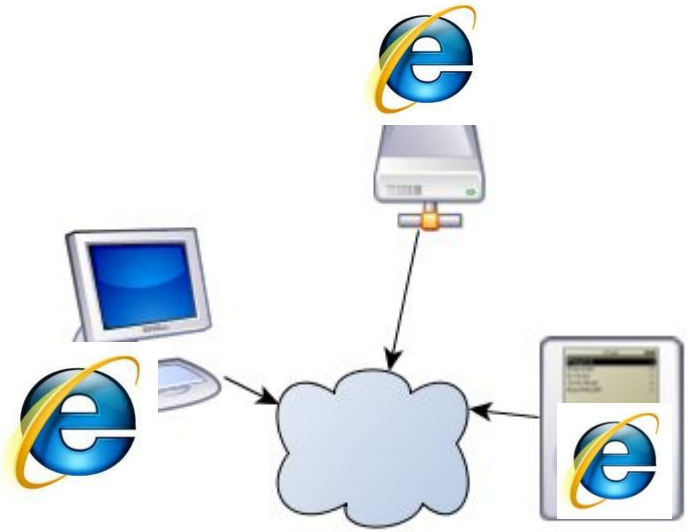
- «Закон управления безопасности информационными технологиями» - закон вступил в силу 01.02.2011
- Единый координирующий центр на базе Института математики и информатики ЛУ - CERT.LV
- Задача - осуществлять превентивные меры против киберпреступников. Задаются минимальные требования безопасности для всех государственных и муниципальных учреждений, а также определяются их действия в экстренных случаях. Закон учитывает директиву ЕС.
- Контакты CERT.LV:
  - 24x7 (тел. 67085858), cert@cert.lv
  - www.cert.lv
  - Общественный портал - www.esidross.lv

Статистика инцидентов за 2011 год



Атаки на облачные сервиса – старые приёмы работают!

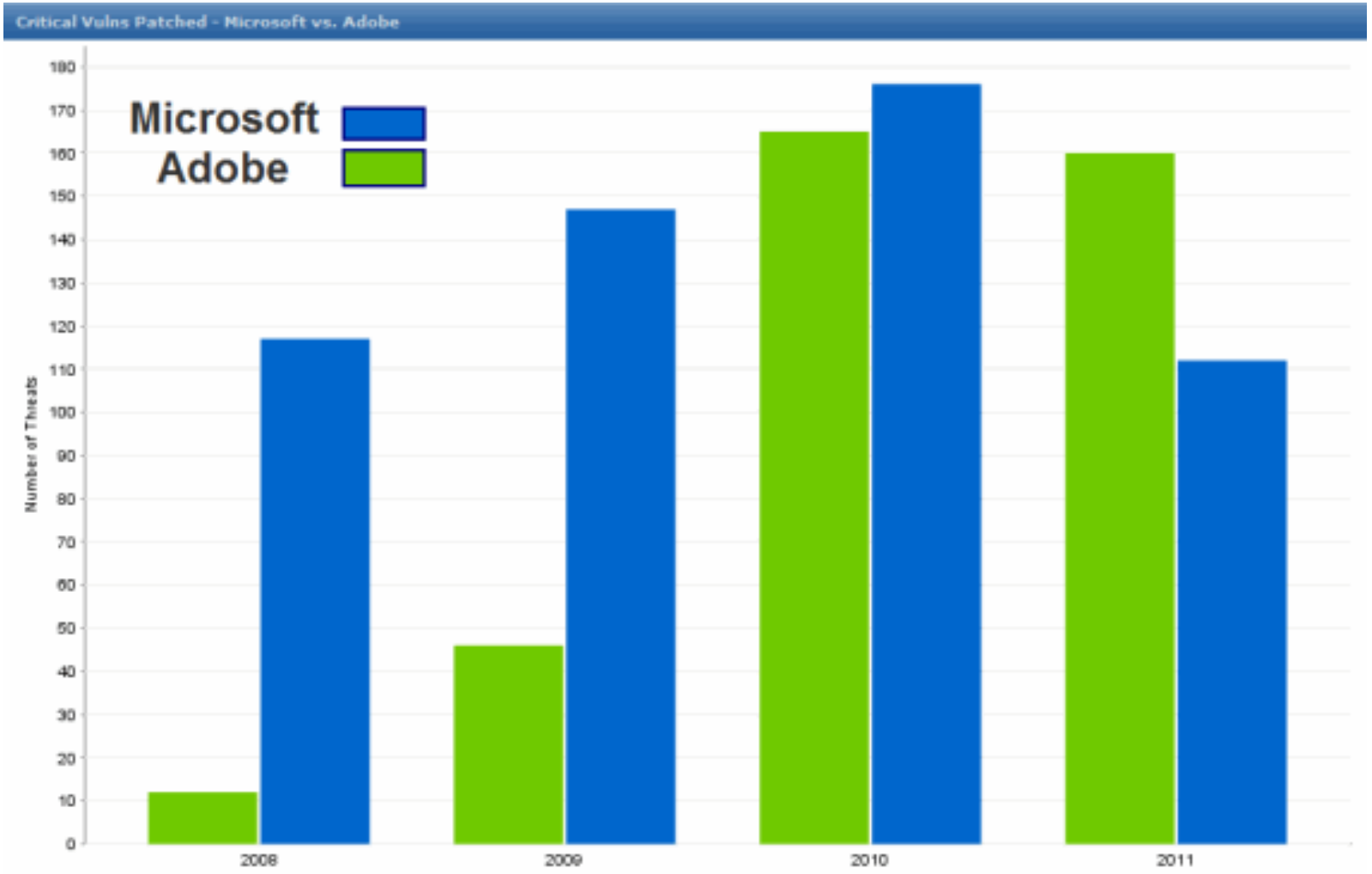
- Интернет браузер – новый компьютер
- Не надо атаковать весь компьютер - полный доступ к данными возможен через браузер!
- Устройство на котором установлен браузер уже не интересно - вся информация и так доступна!



Атаки на облачные сервиса – старые приёмы работают!

- Компьютер клиента - новый сервер
- Всегда - подключен к интернету
- Почти всегда - без обновленного ПО
- Иногда - с широкими правами доступа для пользователя

Атаки на облачные сервиса – старые приёмы работают!



Атаки на облачные сервиса – большая мишень

- 2009 – более 300 документов об бизнес планах TWITTER украдены через Google Apps - причина - лёгкий пароль
- 2010 - Создана программа взлома паролей беспроводной сети на основе Amzon E2 Cloud
- 2011 – Amazon E2 Cloud использован для атаки на Sony PSN
- 2011 – Сервис DROPBOX по ошибке отключил авторизацию на несколько часов - стало возможно скачать любые файлы.

Безопасность данных в "облаке"

- Самое слабое звено – человек!
- Самое неконтролируемое для конечного пользователя - технология
  - Знайте ли бы в какой стане хранится ваше письмо в Google?
  - Каковые последствия будут кораблекрушению в Атлантике?
  - Кто вчера подключался к вашему компьютеру?

- Считайте информацию вашего компьютера публичной :)

  1)если она не зашифрована

  2)если пароль доступа слишком короткий

  3)если ваш компьютер заряжен компьютерным вирусом

Интернет подключение - критичная зависимость

- Большинство компаний намного больше завысит от интернета чем кажется
  - Денежные переводы
  - Базы данных складов
  - Согласование договоров
  - Резервация гостинцы для командировки
- Некоторые виды бизнеса уже не может существовать без интернета
  - интернет порталы
  - сетевые магазины
  - системы резервации билетов
  - предприятия логистики

DOS атака как инструмент шантажа бизнеса

- злоумышленники определяет слабое место:
  - плохо защищен сервер или компьютерная сеть
  - слабые пароли доступа
  - ошибка в коде приложения обработки данных
  - маломощное интернет подключение
- выбирает бремя атаки:
  - рождественская распродажа
  - праздники
  - начало сезона продаж
- производит маломощную атаку, и выходит на контакт со владельцем бизнеса
  - называет "сумму откупа"
  - грозит продолжать атаку

Облачные сервиса - хорошая зашита от DOS шантажа

- Сервера хорошо защищены и вовремя обновлены
- Компетентная техническая поддержка
- Каналы связи с большой пропускной способности
- Вам для работы достаточно маломощного подключения к интернету

Заключение

Если ваша компания подверглась кибер атаке:

- свяжитесь с компетентным и проверенным специалистом
- если нужна консультация или помощь для активного противодействия атаке - свяжитесь с CERT.LV
- оцените урон
- если урон значительный - сообщите об этом в полицию

Спасибо за внимания!

Электронная почта: gints@cert.lv
http://www.cert.lv
http://www.esidross.lv
CERT.LV Twitter: http://twitter.com/certlv