

Сегментированная локальная сеть

Вариант экономии на
закупке дорогостоящей
«песочницы»

Инцидент

- Компьютер Компании после открытия файла электронной почты перестал реагировать на команды Пользователя
- Решение – выключить компьютер и сообщить в отдел ИТ

Этика в работе

- В Компании на регулярной основе с коллегами проводятся беседы с презентацией примеров компьютерных сбоев при воздействии программ – «зловредов»
- Результат – правильно принятое решение в момент инцидента

Последствия

- Данные компьютера ,на момент работы, утеряны
- Компьютеры в локальной сети не пострадали
- Первичный осмотр жесткого диска – файлы зашифрованы неизвестной программой

Электронная почта

- Адресат , отправленного письма, изначально при беглом просмотре оказался известным
- Но только по количеству символов в имени, а изменённый был только один символ

Что делать?

- Перейти на счета и работать без компьютера – так пошутил коллега из коммерческой службы
- Закрывать всем доступ и выделить один компьютер для работы в Интернет – финансисты уже не шутили
- Усилить периметр безопасности сети – предлагает отдел ИТ

Усиливаем периметр сети

- Рассматриваем разные варианты от программных до программно - аппаратных

Тестирование

- Технология «песочница» показала результат своей работы, мы увидели визуально с чем сталкиваемся ежедневно
- Бюджет не рассчитан на такие затраты

Блокировка сети

- Как доступное решение – лишить доступа в Интернет
- Список компьютеров составлен так и не был

Первичные файлы

- Компьютеры разделили по группам обработки принимаемых файлов
- Группы изолировали друг от друга по невидимости в сети

Цель изоляции

- При инциденте под угрозой ограниченная группа компьютеров, а не сеть в целом

Аппаратное решение

- Локальную сеть усилили программируемыми маршрутизаторами
- Создали сегментированную сеть с правилами настроек в маршрутизаторе

В итоге

- Сопоставив экономическую составляющую и требования к работе ЛВС было принято решение по установке дополнительной аппаратной части в Компании.