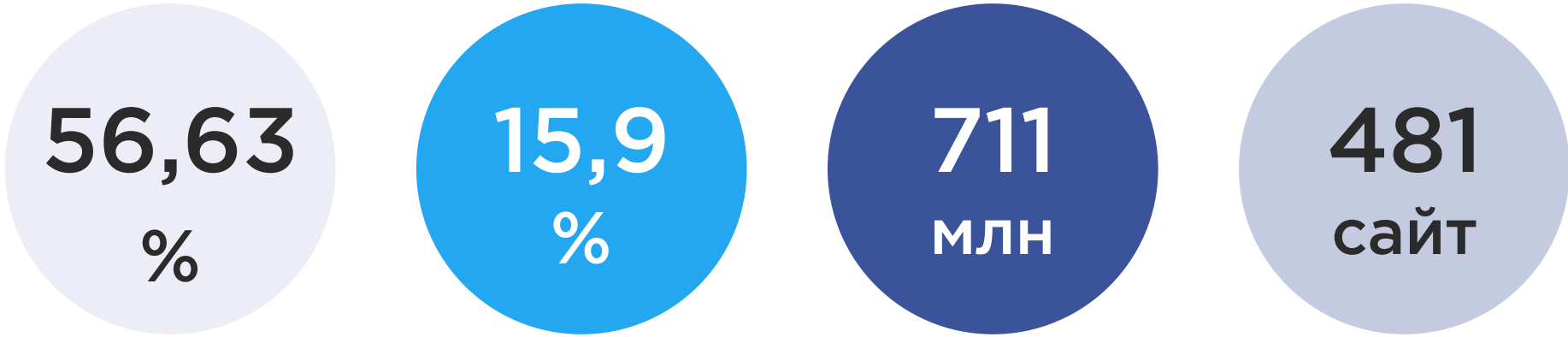
ФИЛЬТРАЦИЯ ПОЧТОВЫХ СООБЩЕНИЙ

НА ОСНОВЕ CISCO ESA И FIREEYE EX

СТАТИСТИКА



доля спама в почтовом трафике

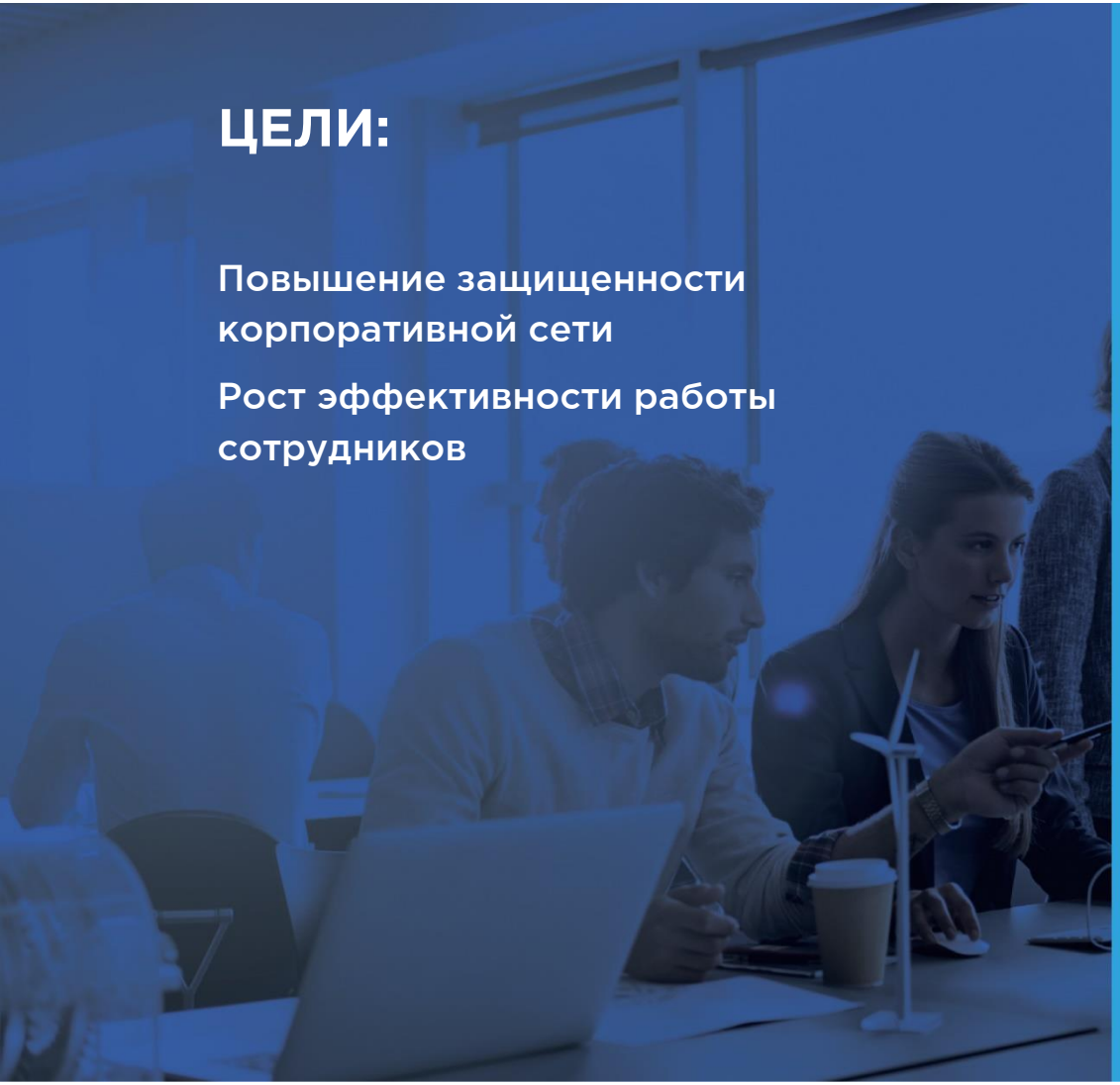
пользователей столкнулись с фишингом

адресов содержалось в базе спам-бота Onliner, рассылавшего электронные письма с трояном Ursnif

используемый мошенниками в фишинг-схемах, выявил ЦБ в 2017 году

** по данным исследования «Лаборатории Касперского» за 2017 г., ФинЦЕРТа ЦБ*

ЦЕЛИ И РЕЗУЛЬТАТЫ



ЦЕЛИ:

Повышение защищенности корпоративной сети

Рост эффективности работы сотрудников

РЕЗУЛЬТАТ:

Снижение рисков ИБ и количества инцидентов, связанных с атаками через почтовые сообщения

Уменьшение нагрузки на технику за счет предварительной фильтрации спама

Экономия времени сотрудников на разбор почтовых сообщений

Сокращение количества писем, попадающих на карантин и последующий анализ сотрудников IT-отдела

Снижение загруженности служб ИБ и IT

МИФЫ И ЗАБЛУЖДЕНИЯ

В наш почтовый сервер уже встроено антиспам-решение, еще одно нам ни к чему

У штатных и бесплатных решений нет гибких настроек: большая доля спама все равно дойдет до пользователей, а важная деловая переписка, наоборот, может быть задержана

Установленные на почтовом сервере накладные антивирусные и антиспам-продукты надежно защищают

Но при этом они требуют дополнительных вычислительных ресурсов. Это критично при росте инфраструктуры. Связка Cisco ESA и Fireeye EX полностью снимает нагрузку с почтового сервера.

У нас уже есть сотрудники, отвечающие за разбор заблокированных сообщений

Отлично, но можно в разы снизить нагрузку на них за счет эффективной фильтрации на основе поведенческого анализа и гибкой настройки правил.
А освободившиеся ресурсы направить на другие направления ИБ.

CISCO IRONPORT ESA: ЗАЩИТА ОТ СПАМА И DLP

Встроенные и настраиваемые политики ИБ

Сигнатурный анализ на основе собственной базы SenderBase

Простое управление и быстрый поиск по нарушениям DLP

Минимальное количество ложных срабатываний

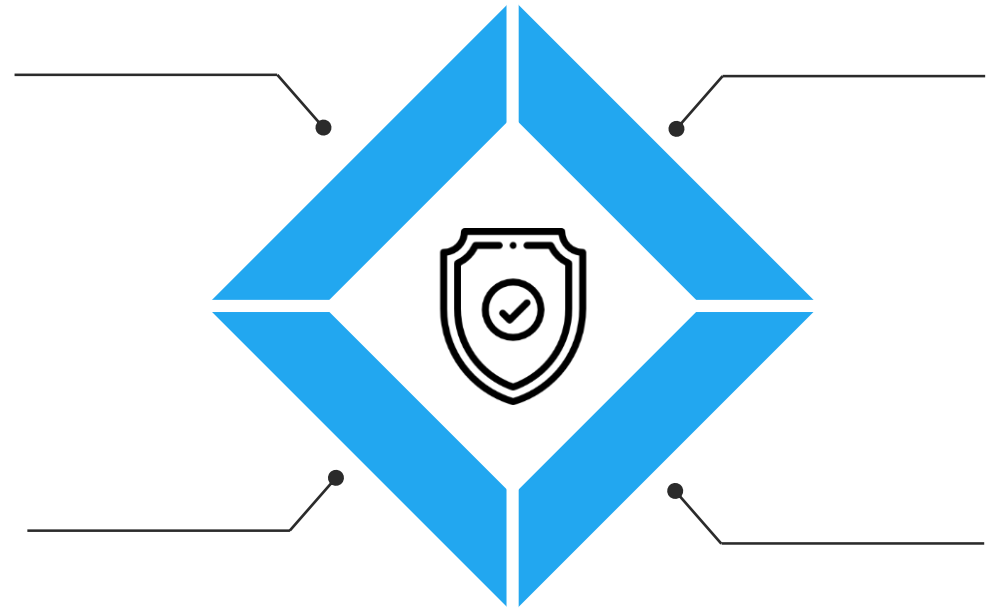
Соответствие нормативам и стандартам (включая PCI DSS)

Высокая производительность шифрования почты (если необходимо)

FIREEYE EX: ЗАЩИТА ОТ НАПРАВЛЕННЫХ АТАК

Анализ вложений на основе безсигнатурной технологии Multi-Vector Virtual Execution (MVX)

Запуск проверки подозрительных вложений во всех видах браузеров и плагинов, включая Reader и Flash



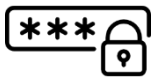
Интеграция с FireEye NX для отслеживания смешанных атак

Динамическое создание профилей угроз

FIREEYE EX: АНАЛИЗ РАЗНЫХ ТИПОВ ВЛОЖЕНИЙ

Все виды опасных расширений, включая EXE, DLL, PDF, SWF, DOC, XLS, PPT, JPG, PNG, MP3 и ZIP/RAR/TNEF-архивы

Перенаправляемые, укороченные и другие адреса



Защищенные паролем вложения

Файлы, загружаемые через ссылки

URL-адреса, встроенные в PDF, документы MS Office, архивы

Скомпроментированные и похожие на фишинговые адреса

ВАРИАНТ ВНЕДРЕНИЯ: ФИЛЬТРАЦИЯ В ОБЛАКЕ

СЕРВИСЫ:

Подключение к фильтрации почты
Предоставление почтового сервера (если необходимо)

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ:

до 150

СРОК ВНЕДРЕНИЯ:

20-40 рабочих дней

ЭТАПЫ ВНЕДРЕНИЯ:

Анализ трафика почтовых сообщений
Проектирование: настройка фильтрации по профилю клиента
Внедрение: изменение настроек SMTP, DNS
Запуск сервиса
Подготовка регламентированной отчетности
Настройка Service Desk (OTRS) для приема сообщений от клиента

ВАРИАНТ ВНЕДРЕНИЯ: В ИНФРАСТРУКТУРЕ ЗАКАЗЧИКА

СЕРВИСЫ:

Развертывание системы фильтрации почты

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ:
от 150

СРОК ВНЕДРЕНИЯ:
3 месяца

ЭТАПЫ ВНЕДРЕНИЯ:

Анализ трафика почтовых сообщений
Анализ почтовой инфраструктуры
Проектирование: настройка фильтрации по профилю клиента
Поставка оборудования
Внедрение: изменение настроек SMTP, DNS
Запуск сервиса
Подготовка регламентированной отчетности (опционально)
Настройка Service Desk (OTRS) для приема сообщений от клиента (опционально)

ПРИМЕР РЕАЛИЗАЦИИ

КОМПАНИЯ А:

финансовая организация,
более 20 лет на рынке,
10 филиалов по стране,
100+ сотрудников

РАБОТЫ:

внедрение CISCO ESA
в дополнение к уже
существующему
антиспам-решению

СРОКИ:

1 месяц

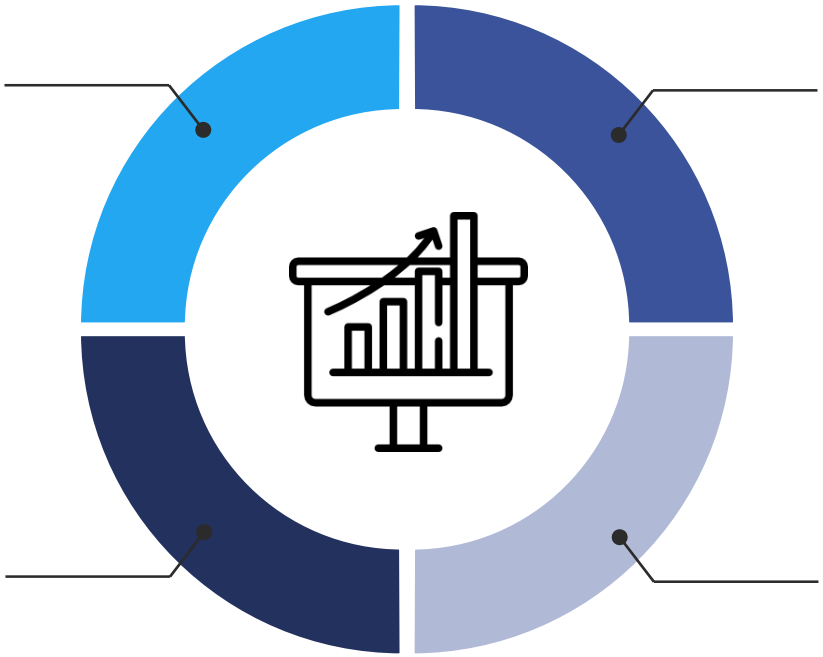
РЕЗУЛЬТАТЫ:

Существенная оптимизация почтового трафика и повышение уровня ИБ. Уже после фильтрации встроенным антиспам-решением благодаря новой системе было выявлено писем (за месяц):

С низкой репутацией	Со спамом	С возможным спамом	С макросами	С опасными вложениями	С опасными ссылками
>8000	**~4000**	**>700**	**~100**	**>30**	**>30**

НАШИ ПРЕИМУЩЕСТВА

Опыт внедрения в крупных компаниях со сложной и разветвленной инфраструктурой



Полный цикл внедрения и сопровождения системы фильтрации почты

Подключение к облаку или создание системы в инфраструктуре заказчика

Поддержка уже функционирующей системы у заказчика

gk-is.ru