

Импортозамещение в ИБ:

сложности и варианты их решения на примере кейсов

Кай Михайлов

руководитель направления
информационной безопасности
ITPROTECT



Импортозамещение в ИБ

Немного занимательных цифр

x3

Увеличилось число запросов
на импортозамещение в 1-2Q
2022

ITPROTECT

30

Зарубежных вендоров ИБ
сегмента ушли из России в 2022
году

Positive Technologies

+20-50%

В среднем увеличились штат и
вложения российских некоторых
ИБ-вендоров в RnD

Опрос вендоров-партнеров

Импортозамещение в ИБ

Немного занимательных цифр

x3

Увеличилось число запросов на импортозамещение в 1-2Q 2022

ITPROTECT

30

Зарубежных вендоров ИБ сегмента ушли из России в 2022 году

Positive Technologies

+20-50%

В среднем увеличились штат и вложения российских некоторых ИБ-вендоров в RnD

Опрос вендоров-партнеров

Основная задача:

вернуть уровень информационной безопасности до того, что был до 24.02

Рынок AntiSPAM

Рассмотрим на примере потоковых антиспам-решений



Рынок отечественных решений не блещет разнообразием (2-3 основных игрока)

Даже на действующих зарубежных решениях не обновляются базы сигнатур

Заказчики привыкли к функционалу и хотят, чтобы замена в точности повторяла старый иностранный продукт



Кейс: Повышение эффективности спам-фильтра

Заказчик: Крупная алкогольная компания

Проблема:

Решение по защите от спама FortiMail перестало обновляться.

В выбранном отечественном решении (Kaspersky Secure Mail Gateway) пока нет всех функций, к которым привык заказчик:

- проверки существования пользователя в домене
- отключения и изменения заголовков писем
- возможности гибкой настройки уведомлений

Решение:

Внедрили KSMG, активировали функционал postfix для проверки существования пользователей, изменили шаблоны конфигурационных файлов для гибкой работы с заголовками, сформировали динамические ссылки для рядового пользователя, пересмотрели правила обработки спама.

Результат

Заказчик оценил удобство работы с порталом самообслуживания для пользователей, снизил нагрузку на внутреннюю службу поддержки.

Уменьшилось количество ложно-положительных срабатываний => администраторам безопасности эскалируются только исключительные случаи, связанные с фишинговыми атаками.



Решение полностью заменило нужный функционал западного антиспама.



Рынок MDM

Текущие сложности

- 1. Иностранные MDM-системы сочетают в себе функционал сразу нескольких классов решений (MDM, MAM и EMM)**
- 2. Российские MDM-системы сосредоточены на более узких задачах, либо:**
 - управление мобильным устройством
 - работа с приложениями и контейнером
- 3. Проксирование приложений до внутренней среды организации обычно осуществляется вне MDM (другим классом решений)**



Кейс: Полный цикл управления мобильным устройством

Заказчик: Химический холдинг

Проблема:

Требуется обеспечить доступ во внутреннюю инфраструктуру с корп. устройств до 5 приложений через сложную сеть и выстроить процесс управления устройствами и приложениями.

Ни одним российским MDM-продуктом такого не решить.

Решение:

Пилотируем решение из связки продуктов:

- MDM SafePhone
- WorksPad
- VPN КриптоПро Ngate

Результат

Заказчик сможет управлять устройствами:

- Выполнять команды (блокировать устройство и его функции, удалять данные и пр.)
- Отслеживать логи и телеметрию, изменять настройки в зависимости от местоположения
- Управлять корп. данными в контейнере, блокировать выгрузку данных наружу
- Предоставлять доступ к инфраструктуре компании из любой точки мира
- Удаленно устанавливать и обновлять приложения и пр.



Получилось создать полноценное MDM-решение на основе 3х продуктов

Рынок AntiAPT

Текущие сложности

- 1. Сильная зависимость от вычислительных мощностей**, сложности с поставкой оборудования
- 2. Двойная виртуализация решает проблему, но создаёт новые:**
 - сложнее скрыть факт исследования от сканируемой вредоносной программы
 - усложнение архитектуры и внезапные технические сложности
 - вендоры пока ориентированы на зарубежные гипервизоры
- 3. Отсутствие образов российских ОС в большинстве российских песочницах** (отдельных или модулей)

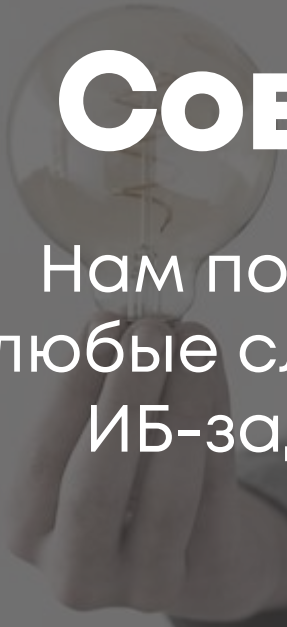


Общий «недуг» отечественных СЗИ

Часто
сложное и
неудобное
администрирование



Чем мы можем помочь



Совет?

Нам полезны
любые сложные
ИБ-задачи

Пишите,
звоните!



2-6 мес

Бесплатных лицензий
для тестирования
российских ИБ-
продуктов

itprotect

ЗАЩИЩАЕМ, ОПЕРЕЖАЯ УГРОЗЫ

Остались вопросы?

Кай Михайлов

k.mikhaylov@itprotect.ru

+7 977 436 8658



Новости рынка ИБ и
рекомендации

