Мир никогда уже не будет прежним:

Что стало с информационной безопасностью и каких изменений ждать в будущем.

Руководитель отдела ИБ Лаборатории Касперского

Андрей Евдокимов

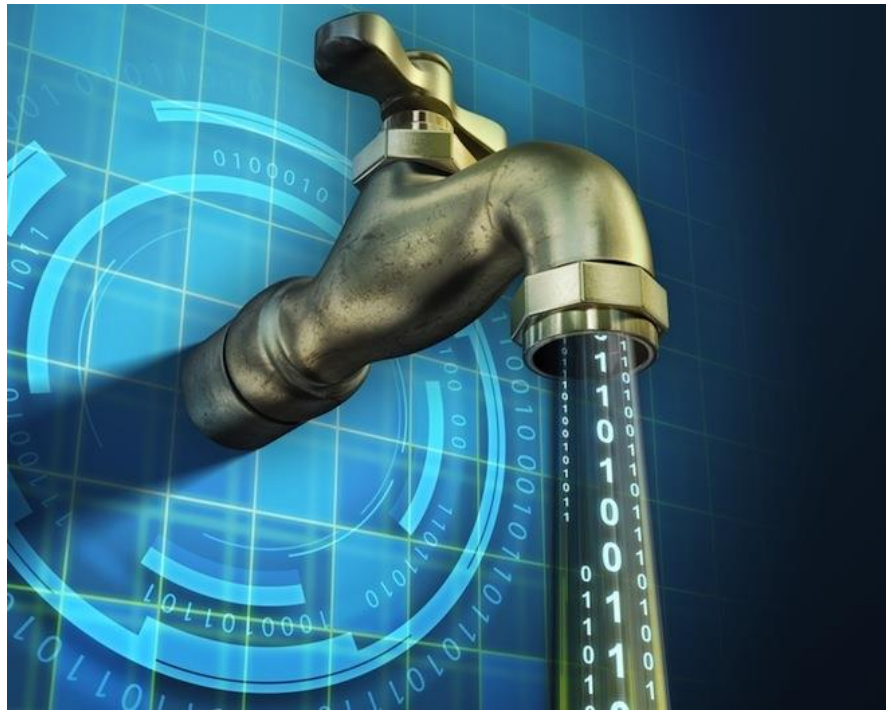
Необходимость быстро адаптироваться в условиях сложно-прогнозируемых изменений

Хит-парад «Атаки на пандемии»

Меры защиты

- Anti DDoS
- Использование распределенных систем

Хит-парад «Атаки на пандемии»



Утечки конфиденциальной информации из-за некорректного использования облачных сервисов, ошибок при интеграции с внешними сервисами, при разделении ответственности с подрядчиками

Меры защиты

- Вовлечение ИБ в создание и изменение ИТ систем и сервисов;
- Контроль «теневого ИТ»;
- Требования к подрядчикам и вендорам, контроль их выполнения;
- Безопасность облачных сервисов: встроенные средства провайдеров, управление доступом на основе принципа минимальных привилегий, контроль настроек;
- Настройка ОС и ПО (Hardening).

Хит-парад «Атаки на пандемии»

Атаки на web-сервисы с целью НСД к данным

Меры защиты

- Безопасная разработка и участие ИБ в создании и изменении web-сервисов;
- Сегментирование сети, управление установкой обновлений, настройка ОС и ПО (Hardening);
- Сканеры уязвимостей и контроль устранения уязвимостей;
- Web application firewall;
- Управление событиями и инцидентами ИБ (SIEM + EDR + SOC.

Хит-парад «Атаки на пандемии»

Атаки на цепочку поставок (Supply chain attacks)

Меры защиты

- Требования к подрядчикам и вендорам, контроль их выполнения;
- Контроль «теневого ИТ»;
- Многоуровневая защита с использованием решением различных вендоров;
- Управление доступом подрядчиков на основе принципа минимальных привилегий.

Хит-парад «Атаки на пандемии»

Атаки с использованием вредоносного ПО

Меры защиты

- Базовые средства: AAA (аутентификация, авторизация, учет), сегментирование сети, управление установкой обновлений, настройка ОС и ПО (Hardening);
- Защита компьютеров и серверов: KES + EDR + Sandbox;
- Защита почтовых серверов: Kaspersky security for Exchange + Sandbox + Hardening почтовых серверов;
- Защита от APT (KATA + Sandbox + MDR);
- Управление событиями и инцидентами ИБ (SIEM + EDR + SOC);
- Сканеры уязвимостей и контроль установки обновлений;
- Безопасный удаленный доступ и контроль подключаемых устройств: VDI, VPN, NAC.

Хит-парад «Атаки на пандемии»

Атаки на интерфейсы удаленного доступа, уязвимости в корпоративных системах (выявление уязвимых RDP, подбор и перехват паролей, выявление SMB опубликованных в Интернет и т.п.). Цель – компьютеры удаленных сотрудников и новые каналы доступа в сеть

Меры защиты

- Безопасный удаленный доступ: VDI, VPN, NAC;
- Базовые средства: AAA (аутентификация, авторизация, учет), сегментирование сети, управление установкой обновлений, настройка ОС и ПО (Hardening);
- Сканеры уязвимостей и контроль устранения уязвимостей.

Хит-парад «Атаки на пандемии»

Фишинговые атаки и атаки направленные на компрометацию корпоративной переписки (business email compromise)

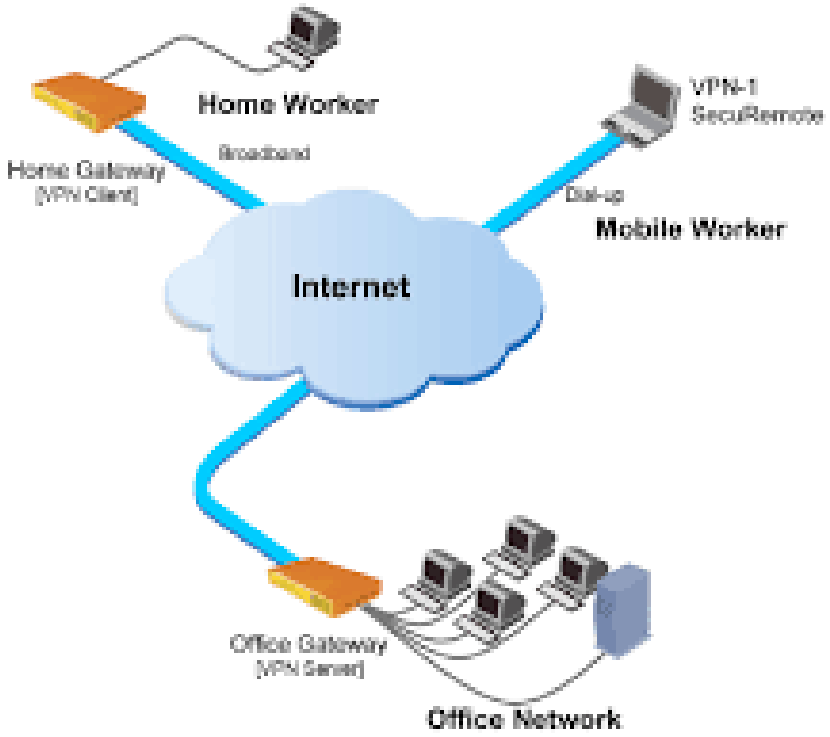
Меры защиты

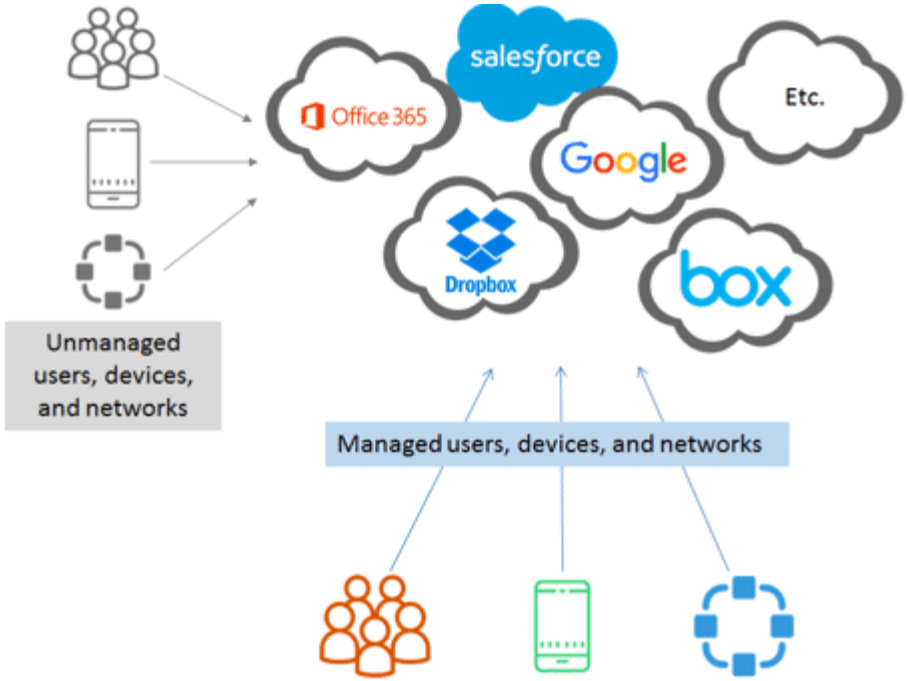
- Обучение сотрудников;
- Защита почтовых серверов: Kaspersky security for Exchange + Hardening почтовых серверов;
- Защита компьютеров KES + EDR;
- Управление событиями и инцидентами ИБ (SIEM + EDR + SOC).

Востребованные бизнесом технологии

- Машинное обучение и системы искусственного интеллекта;
- Профилирование и поведенческий анализ клиентов и пользователей, интеграция с внешними аналитическими сервисами;
- Частные и публичные облачные сервисы;
- Интеграция бизнес-систем с социальными сетями;
- Виртуализация серверов, контейнеризация приложений и сервисов;
- Использование личных устройств и технологий, к которым привык (BYOT & BYOD);
- Технологии, обеспечивающие мобильность сотрудников;
- Рабочие места как сервис (DaaS), виртуальные рабочие места (VDI).

Больше нельзя не замечать «облаков»





Требования к информационной безопасности

Обеспечение возможности быстрой и безопасной (на основе управления рисками) трансформации бизнеса в условиях внешних изменений и изменений потребностей клиентов.

Спасибо за внимание!