Разработка с BYOD: как обеспечить безопасность продуктов

настоящие возможности

росбанк 30 лет

Спикер

Илья Шмаков

Заместитель начальника отдела Информационной Безопасности управления рисками

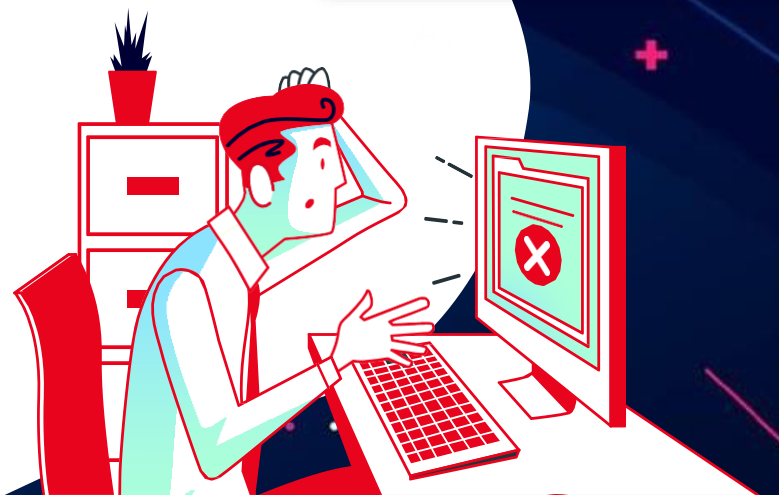
- **Аналитик рисков** ИБ, **сертифицированный** DASA DevOps Product Owner, devops-инженер
- **Более** 8 лет работы в разработке ПО в части **DevSecOps**
- Работает **в сфере обеспечения ИБ** для продуктовой разработки в **BI, E-Commerce, Supply Chain, Cryptocurrency, GameDev**
- Проработал **двухэтапную защиту multisig** с учетом распределенного резерва согласно **эскроу-схемы** при проверке **горячего хранения** для Stable-коинов как **отдельного продукта**
- **Основатель и лидер** сообщества **FinDevSecOps** на базе **АФТ** и **MOEX** (при взаимодействии с **ЦБ**)
- **Ведет** курсы на платформе **InSeca.tech**
- **Руководит группой** офицеров информационной безопасности, развивает **DevSecOps** в банке

росбанк

Сервис Happy Developer

Сервис удаленного подключения сотрудников Банка и подрядных организаций с личных устройств (BYOD) к ограниченному списку разрешенных ресурсов Банка в тестовой, сертификационной (v1.0) и продуктивной среде (v2.0).

Доступ осуществляется из сети общего пользования (из сети Банка услуга недоступна).



росбанк

Что даёт командам?

1. Удобная поставка продуктов по бизнес задачам
2. Сдерживание Time to Market
3. Контроль Service Relationship Management и оптимизация
4. Стандартизация процессов работы с подрядчиком и получения их поставок во внутренний контур
5. Позволяет ориентироваться на метрики ценности
6. Возможность управления изменениями и SoD
7. Контроль ИБ со стороны разработки продуктов и процессов
8. Формирование требований ИБ под публикуемые сервисы
9. 

росбанк

Что даёт в контроле?

Применяемый инструментарий ИБ

- Web DLP
- Anti-APT
- CAB3 на endpoint HD (BYOD)
- PIM/PAM
- IDM
- WAF с SSL
- Sandbox Inspection
- ASOC - Monitoring & Analysis

Основные контроли

- Автоматизированный контроль состояния из периметра
- DLP на endpoint BYOD
- UBA системы для обнаружения искажений поведения пользователей
- 2FA с ОТП перед VPN
- Ограничение и контроль USB
- Proxy

Решением по контролю является SoD (segregation of duties или разделении прав доступа) для контроля привилегированных пользователей в рамках PIM/PAM и модели *Maintain users & Assign roles/profiles to users, etc.*

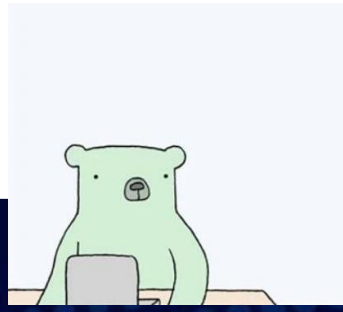
Базируется проработка на базе Ruleset, рисков комбинации функциональных разрешений SoD, uni-SoD, то есть кастомизация решения.

Аналогично ограничиваются привилегированные пользователи к возможности подключения к HD.

росбанк

Требования ИБ при публикации в HappyDev

- ASA, SSF на систему есть и они актуальны
- Система не содержит конфиденциальную информацию (БТ, ПДн, card data, С3 и С2 информацию)
- Система сканируется, проведен пентест, уязвимости закрыты
- Система поддерживает https с нужными алгоритмами
- Система находится в отдельном сегменте DMZ типа
- Консоль администрирования может быть заблокирована на WAF с SSL Inspection
- Реализовано бэкапирование системы
- Подготовлено инфраструктурное ТР согласно требованиям ДИБ
- Выполнение работ выполняется во внерабочее время



росбанк

Подход к управлению рисками

в процессах Quality Gate

1. **Анализ взаимосвязи безопасности данных с бизнес-ценностью продукта** и устранением уязвимостей supply-chain

2. **Разработка корректируется на ценности продукта** конечному пользователю исходя из повышение безопасности, вследствии устранения уязвимостей. Влияют условия принятия рисков ИБ и возможность их минимизации

3. **Разработка с учетом выполнения мер по минимизации значимых рисков** перед выпуском в промышленную среду (PRE-условия) или после с последующим контролем (POST-условия)

4. **Quality Gate контролирует технологически конфигурационные файлы**

Повышение эффективности управления рисками и уязвимостями

росбанк

Наши рекомендации

1

- Правильно выстроенный процесс важнее инструментов
- Не внедряйте всё и сразу — начните с того, что уже есть, и двигайтесь исходя из потребности: тип интеграции, назначение, бизнес-процесс
- Функциональные дефекты и уязвимости равны

2

- Выращивайте в своих командах **Security Champions** и задействуйте в процессе разработки — это повысит поток ценности увеличивая безопасность продукта,
- Помните, что качество продукта — это общая цель
- Важнее люди, а не процесс
- Разделяйте влияние обособленных команд

3

- Автоматизируйте по максимуму – **Infrastructure-as-a-Code** to **Everything-as-a-Code**
- Выбирайте процессы и инструменты, подходящие именно для вашего продукта
- Делайте упор на метрики здоровья и зрелости продукта, - нивелируйте **legging**

росбанк

Вопросы & ответы

настоящие возможности

росбанк 30 лет