www.pwc.ru/cybersecurity

Обзор подходов к управлению уязвимостями и угрозами

Pentesting vs Red teaming

Роман Чаплыгин

pwc

Драйверы развития TVM

Внешнее регулирование и рекомендации

- Положение Банка России от 9 июня 2012 г. № 382-П
- TIBER-EU 2018 от European Central Bank
- NYCRR Part 500 от New York State Department of Financial Services
- SRD TR 01 2014 от Monetary Authority of Singapore
- CBEST Implementation Guide от Bank of England

Внутренние факторы

- Цифровизация и необходимость постоянного и глубоко анализа уязвимостей
- Agile, скорость вывода новых и внесения изменений в текущие цифровые продукты и услуги
- Внимание к кибер рискам со стороны ТОП-менеджмента и необходимость усиления превентивной защиты
- Распространение моделей BYOD и постоянно изменяющийся ландшафт инфраструктуры при применении облачных технологий и контейнеризации.

Pentest vs Red teaming (1/2)

	Pentest	Red teaming
	• Фиксированная область проекта, определенные внешние/внутренние системы и приложения	• Все доступные активы компании
	• В зависимости от типа проекта, возможно наличие легитимного доступа к тестируемой инфраструктуре	• Данные для доступа к анализируемым приложениям и системам не предоставляются
	• Оповещение внутренних служб ИТ и ИБ зависит от типа проекта и модели взаимодействия	• Оповещение внутренних служб ИТ, ИБ и анализа событий не предусмотрено
	• Время проведения обычно согласовывается заранее и совпадает с рабочими часами работников организации	• Проведение атаки возможно в любое время
	• Средняя продолжительность активной фазы – 1-2 недели	• Эксплуатация доступных векторов осуществляется итерационно, атака может развиваться в течение нескольких недель и даже месяцев

Pentest vs Red teaming (2/2)

	Pentest	Red teaming
	• Использование основных методологий: OWASP, OSSTMM, EC-Council, WASC, NIST…	• Методология и инструментарий определяется в зависимости от обнаруженных активов и систем
	• Возможно проведение на различных этапах жизненного цикла системы и уровне зрелости процессов ИБ	• Рекомендовано для организаций с развитыми процессами обеспечения ИБ и ИТ (особенно внесения изменений и управления обновлениями)
	• Осуществляется проверка осведомленности пользователей	• Осуществляется проверка осведомленности и поведения пользователей и реакции подразделений ИТ и ИБ
	• Осуществляется поиск вектора атаки, позволяющего осуществить успешную атаку и получить доступ к целевой системе/данным	• Оценивается готовность организации к обнаружению и отражению таргетированных атак, анализ зрелости процессов реагирования на инциденты
	• Результат проекта – рекомендации по устранению выявленных уязвимостей	• Результат проекта – рекомендации по устранению выявленных уязвимостей и улучшению алгоритмов и процесса обнаружения и реагирования на инциденты

Сценарии для тестирования

Эксплуатация уязвимостей внешних сервисов	Фальсификация и клонирование пропусков
Эксплуатация уязвимостей внутренних сервисов	Размещение закладных устройств в переговорных
Проведение атак на мобильные устройства	Попытки преодоления сетевого периметра из общедоступных помещений
Распространение зараженных носителей информации	Проведение фишинговых компаний и использование социальной инженерии
Попытки преодоления пунктов охраны и приёмных	Фиксация времени реагирования и мер, принятых службами ИТ, ИБ и анализа инцидентов

Эволюция TVM

Управление обновлениями	Инструментальное сканирование	Тестирование на проникновение	Red Teaming	Intelligence-led cyber security testing / red teaming
Поиск данных о обновлениях в ручном режиме или на основе подписок	Выявление активов и обнаружение уязвимостей осуществляется системами инвентаризации и анализа защищенности	Имитация действий внешнего / внутреннего нарушителя Поиск вектора, позволяющего нанести ущерб компании Эксплуатация обнаруженных уязвимостей	Анализ периметра и защищенности инфраструктуры, оценка уровня осведомленности пользователей и готовности компании к обнаружению и отражению внешних и внутренних атак Разработка рекомендаций по совершенствованию систем и процессов ИБ	Имитация действий злоумышленников, воспринимаемых государственными и коммерческими разведками в качестве реальных источников угроз для системных финансовых организаций. Анализ защищенности, основанный на оценке рисков, присущих данной отрасли, используемым технологиям и ценностям компании.

Компетенции PricewaterhouseCoopers

Penetration Testing	Cyber Security Incident Response	STAR (Simulated Targeted Attack & Response) Penetration Testing	CBEST Approved Penetration Testing Provider	STAR Threat Intelligence	CBEST Approved Threat Intelligence Provider

https://www.crest-approved.org/membercompanies/pwc/index.html

Тестирование на проникновение и анализ уязвимостей в рамках 382-П

Указание ЦБ РФ от 7 мая 2018 г. N 4793-У вводит новые требования к обеспечению защиты информации в Положение Банка России от 9 июня 2012 года N 382-П и обязывает банки производить **тестирование на проникновение (пентест) и анализ уязвимостей*** информационной безопасности.

Видение рынка и новые вызовы	Рекомендации PwC
Под действие требований попадают автоматизированные банковские системы, системы дистанционного банковского обслуживания, а также информационная инфраструктура	Анализ уязвимостей необходимо проводить для систем Банк-Клиент (ДБО), тогда как тестирование на проникновение должно проводиться для инфраструктуры (сервера, сетевое оборудование), на которой функционирует система ДБО
Необходимо сертифицировать систему дистанционного банковского обслуживания во ФСТЭК	В случае если система приобретена у подрядчика, можно попросить его сертифицировать данную систему, или провести анализ уязвимостей и оценку по требованиям ОУД 4 (ГОСТ 15408). Кроме того, регулятор подготавливает профиль защиты , на основании которого необходимо будет провести оценку по ОУД 4
В случае если в работе Банка используются мощности иностранной компании необходимо тестировать на проникновение и сертифицировать систему (ДБО), которая находится в другой стране	Деятельность зарубежной компании находятся вне юрисдикции регулятора, однако, необходимо построить отлаженный процесс управления уязвимостями и быть готовым, в случае проверки, продемонстрировать его функционирование
Многие Банки ни разу не проводили тестирование на проникновение и не представляют как это реализовать и какие результаты получат	На начальном уровне можно использовать сканеры уязвимостей и базовые техники тестирования на проникновение, также следует сформировать процесс управления уязвимостями и постепенно его развивать
У Банка отсутствует понимание того, как и на основании какой методики проводить тестирование на проникновение и анализ на уязвимостей	Регулятор не накладывает требования к подходу проведения тестирований на проникновение, но в данном вопросе мы рекомендуем руководствоваться лучшими практиками (OWASP, STRIDE, WASC, EC-Council)

Дополнительными источниками и примерами международных практик по тестированию защищенности являются:

- *CBEST Intelligence-Led Testing (UK)*
- *TIBER-EU FRAMEWORK (EU)*

* Тестирование на проникновение и анализ уязвимостей информационной инфраструктуры необходимо провести до 01 июля 2019 г. Анализ уязвимостей и оценку ДБО по требованиям ГОСТ 15408 необходимо провести до 1 января 2020 года.

Спасибо!

Роман Чаплыгин
PwC, Директор

Mob.: +7 (903) 272 1620
E-mail: roman.chaplygin@pwc.com