ScienceSoft

Professional Software Development

Как снизить риски?
Эффективность ИБ глазами нападающего

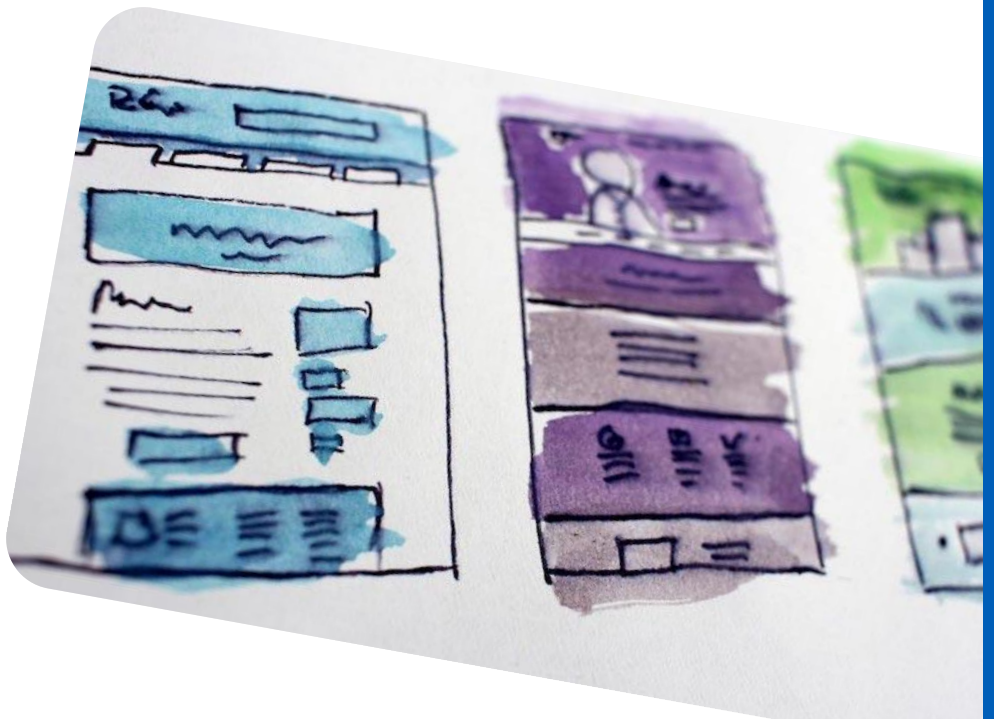
Немного о себе

Кто: Владислав Мурашко
Компания: ScienceSoft
Чем занимаюсь: пентестинг (тестирование безопасности, в том числе развитие направления в рамках компании), консалтинг в сфере ИБ
Опыт: с 2011 года
Сертификации: CEH
Кроме этого: SIEM (ScienceSoft SIEM, IBM Qradar) - опыт интеграции и настройки, работа с инцидентами

Содержание

Как снизить риски? Эффективность ИБ глазами нападающего

- Как помогают пентесты ?
- Зачем нужен SIEM ?
- Как снизить риски ?

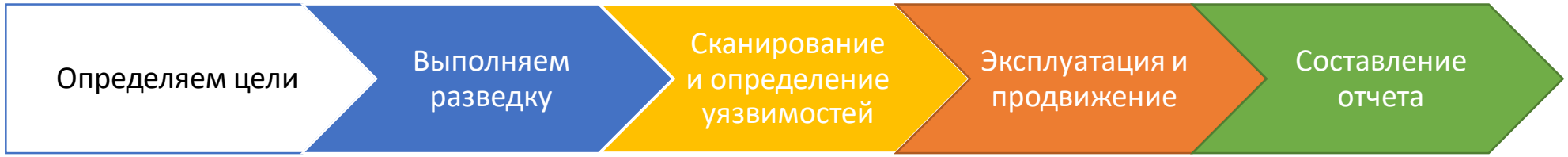


Как помогают пентесты

Что такое пентесты и для чего они нужны

- **Пентестинг (Penetration Testing) –** практика тестирования компьютерных систем, сетей, приложений на наличие уязвимостей и определение уровня осведомленности сотрудников о возможных киберугрозах и корректного реагирования на них.

- **Для чего нужны:**
  - Один из способов нахождения слабых мест в сетевой инфраструктуре компании
  - Один из способов проверки уровня подготовки сотрудников
  - Соответствие требованиям регуляторов (PCI-DSS, HIPAA, GDPR и др.)



Как помогают пентесты

Какие бывают модели пентестов и что они выявляют

Черный ящик

- URL / IP или имя компании
- Отсутствие доступов
- Чаще относится к внешнему периметру

Серый ящик

- Полный список тестируемых целей, частичное раскрытие информации о них
- Могут предоставляться ограниченные доступы (тестовые учетные данные)
- Применимо для анализа защищенности внешнего периметра и внутренней инфраструктуры

Белый ящик

- Полное раскрытие информации (включая политики или документацию)
- Все уровни доступов
- В том числе анализ кода

Помогают выявлять:

- ❑ Уязвимости
- ❑ Ошибки конфигурации
- ❑ Утечки информации
- ❑ Многое другое...

Как помогают пентесты

Мировые стандарты и классификации

Как помогают пентесты

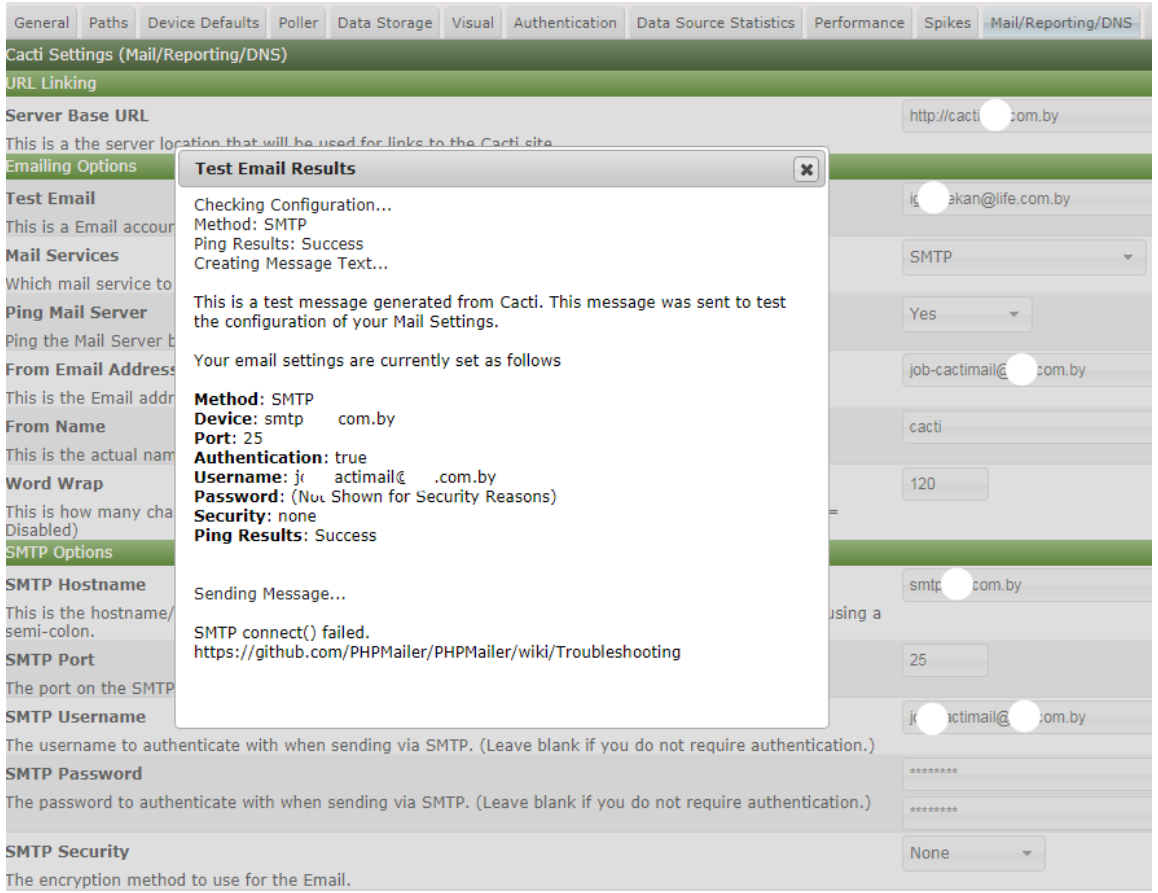
Немного примеров и статистики

Читательница: «Проверяю баланс карточки, а там не хватает 600 рублей, поменяла карту — и кто-то стал пользоваться ею снова»

Минчанин: «Банк не вернул украденные с карточки почти 50 миллионов, потому что я не позвонил им в течение часа после кражи»

Мобильное приложение ставит под угрозу деньги клиентов. Пользователи попадают не в свои, а в чужие личные кабинеты, сообщает телеграм-канал .

```
11.     stage('Checkout branch') {
12.         steps {
13.             echo "Checking out branch ${GIT_BRANCH_LOCAL}     "
14.             git branch: "${GIT_BRANCH_LOCAL}", credentialsId: '37b    5-90f4-    )-8f15-5f    5af542', url: 'git@srv-gitlal
main.velcom.by:d    l_v/ch    )t-callback-service.git'
```



Очередной "развод": у Беларусбанка появился фейковый ...
https://sputnik.by › society › Ocherednoy-razvod-u-Bela... ▾ Translate this page
Feb 20, 2019 - Неизвестные **взломали** страницу Следственного комитета в ... с этого аккаунта они отправляли клиентам **Беларусбанка** сообщения о ...

Источник: Google, GitHub, и др.

Как помогают пентесты

Немного примеров и статистики

География атак банковского вредоносного ПО, второй квартал 2019 года *(скачать)*

TOP 10 стран по доле атакованных пользователей

	Страна*	%**
1	Беларусь	2,0
2	Венесуэла	1,8
3	Китай	1,6
4	Индонезия	1,3
5	Южная Корея	1,3
6	Кипр	1,2
7	Парагвай	1,2
8	Россия	1,2
9	Камерун	1,1
10	Сербия	1,1

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (меньше 10 тысяч).

** Доля уникальных пользователей «Лаборатории Касперского», подвергшихся атакам банковских троянцев, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.

Источник: https://securelist.ru/it-threat-evolution-q2-2019-statistics/94476/

Как помогают пентесты

Немного примеров и статистики

TOP 10 стран по доле пользователей, атакованных майнерами

	Страна*	% пользователей, атакованных майнерами**
1	Афганистан	10,77%
2	Эфиопия	8,99%
3	Узбекистан	6,83%
4	Казахстан	4,76%
5	Танзания	4,66%
6	Вьетнам	4,28%
7	Мозамбик	3,97%
8	Украина	3,08%
9	Беларусь	3,06%
10	Монголия	3,06%

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (менее 50 000).

** Процент уникальных пользователей, компьютеры которых были атакованы майнерами, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.

Источник: https://securelist.ru/it-threat-evolution-q2-2019-statistics/94476/

Как может помочь SIEM

Для чего нужны SIEM системы и как их применять

Нужны для:

- Сбора, анализа и хранения логов
- Выявления инциндентов
- Реагирование на инциденты
- Прохождения аудитов
- Организации своего SOC
- …

Можно применять с:

- DLP системами
- IDS/IPS системами
- Сканерами уязвимостей
- Системами СКД / CCTV
- Системами разведки угроз
- …

Как может помочь SIEM

Несколько примеров из нашего опыта

- Активности сотрудников (уволенные, в отпусках)
- Забытые системные учетные записи
- Попытки записи информации на HDD (и выноса ее)
- Попытки установки кейлогеров
- Попытки прохода через турникеты/камеры
- Мониторинг исходящего трафика:
  - Использование майнеров в рабочей инфраструктуре
  - Попытка слития данных на сторонние хранилища
  - Активности сотрудников в течении дня и др.

Как снизить риски ?

Угрозы бывают не только внешние но и внутренние
На постоянной основе рекомендуется выполнять:

Мониторинг специализированных ресурсов

Тестирование безопасности (Penetration Testing, VA)

Использование SIEM и других вспомогательных систем

ScienceSoft
Professional Software Development

СПАСИБО
ЗА ВНИМАНИЕ!

www.scnsoft.by | www.scnsoft.com