Threat modelling

powszechnie znany, ale rzadko używany

Adrian Sroka

Co chcemy osiągnąć?

Jak najlepiej i jak najmniejszym kosztem zabezpieczyć tworzone przez nas rozwiązania

Bezpieczeństwo w SDLC

Planowanie	Assessmenty
Projektowanie	Zero trust
Programowanie	Code review Statyczna analiza
Testy	DAST IAST
Wdrożenie	Testy penetracyjne
Operacje	Firewall Hardening
Monitoring	SIEM

Bezpieczeństwo w SDLC

Planowanie	Assessmenty
Projektowanie	Zero trust Threat modelling
Programowanie	Code review Statyczna analiza
Testy	DAST IAST
Wdrożenie	Testy penetracyjne
Operacje	Firewall Hardening
Monitoring	SIEM

Modelowanie zagrożeń

Praktyka identyfikowania i priorytetyzacji potencjalnych zagrożeń tworzonych przez nas rozwiązań

Cele

- Znajdowanie luk bezpieczeństwa
- Zrozumienie wymagań bezpieczeństwa

Kto może stosować?

Zespoły, które tworzą rozwiązania

- Zespół deweloperski
- DevOps
- Operacje

Modelowanie zagrożeń w życiu codziennym

Jazda samochodem po zaśnieżonym mieście

- Jakie jest ryzyko poślizgu?
- Czy ktoś może wybiec na ulicę?
- Czy na skrzyżowaniu nic nie jedzie?
- Czy nie jadę zbyt szybko?

Modelowanie zagrożeń jest jak sprawdzanie oleju w samochodzie przed dłuższą wyprawą

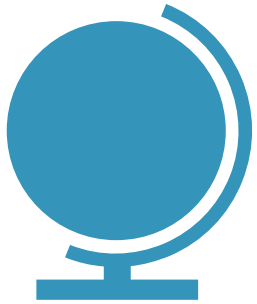
Korzyści z modelowania zagrożeń

- Programiści
  - Nauka bezpieczeństwa
  - Lepsze zrozumienie systemu
  - Wskazówki do dewelopmentu
- Testerzy
  - Możliwość testowania zidentyfikowanych zagrożeń
- Analitycy
  - Możliwość dokumentacji procesu
- Architekci
  - Możliwość zmapowania zagrożeń na inne systemy

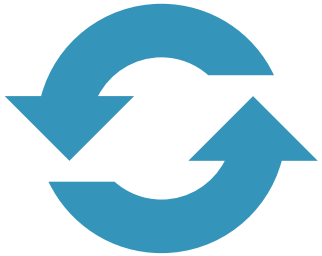
Jak dobrze robić modelowanie zagrożeń?

- W odpowiednim momencie
- W odpowiednim gronie
- Tak, żeby jak najmniej przeszkadzało w procesie
- Dostosowując do poziomu zespołu

Rodzaje modelowania zagrożeń



Globalne



Iteracyjne
- w sposób ciągły

Globalne modelowanie zagrożeń

JEDNORAZOWO

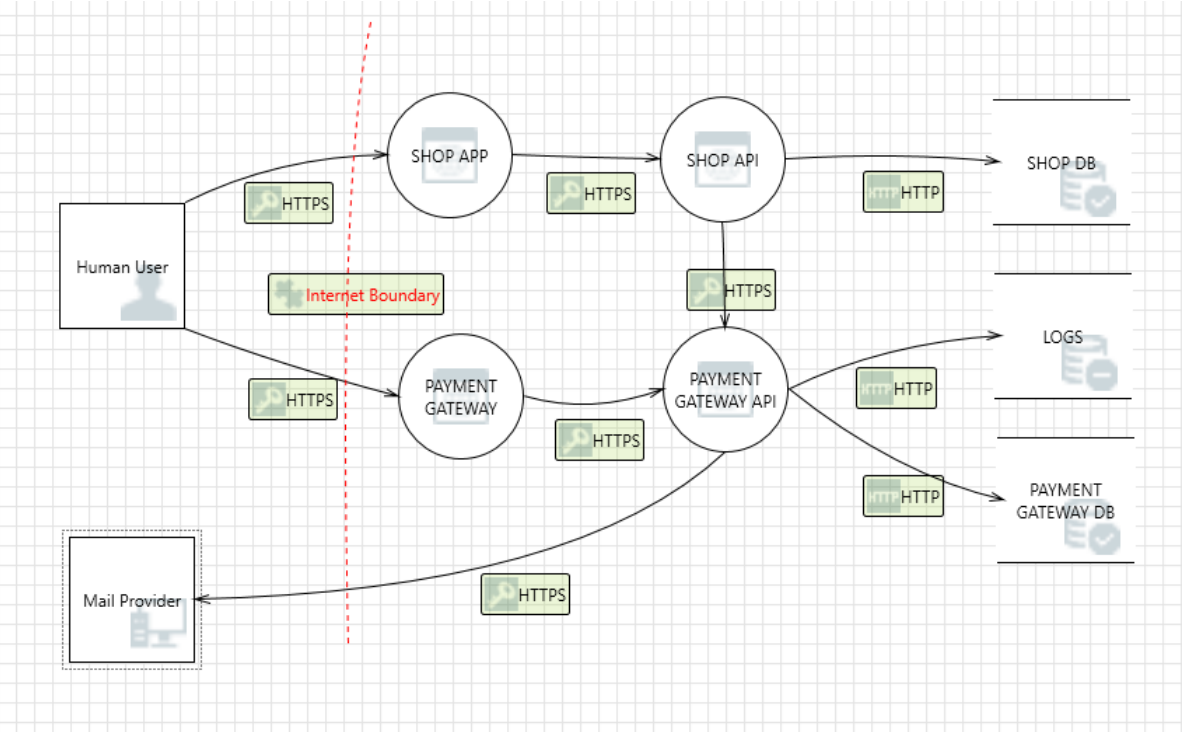
ANALITYK
ARCHITEKT
DEVOPS

Globalne modelowanie zagrożeń

- Co budujemy?
- Co może pójść nie tak?
- Plan mitygacji
- Walidacja planu

Rysujemy diagram

- Data Flow Diagram
- Przepływy
- Komponenty
- Inny



Co jest potrzebne:

- Usługi
- Przepływy danych
- Bazy danych
- Co jest zewnętrzne/wewnętrze

Globalne modelowanie zagrożeń

- Co budujemy?
- Co może pójść nie tak?
- Plan mitygacji
- Walidacja planu

STRIDE

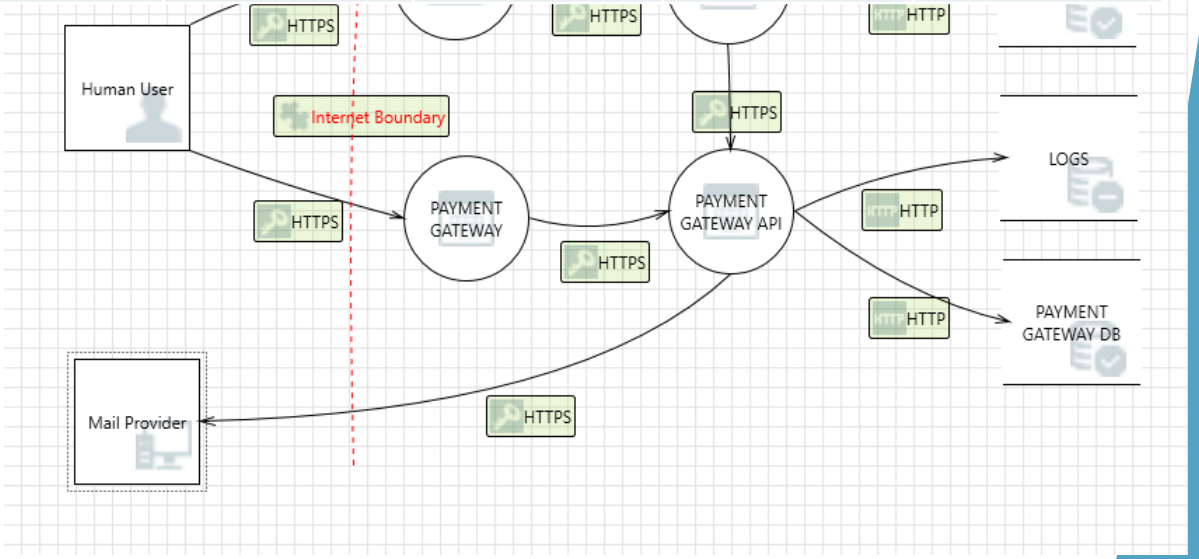
Zagrożenie	Definicja	Przykłady	Mitygacje
Spoofing	Podszywanie się pod kogoś innego	Kradzież tokenu	Hasła
Tampering	Zmiana danych lub kodu	Zmiana ceny podczas płatności	Uprawnienia Walidacje Podpisy
Repudiation	Nie przyznanie się do wykonania akcji	Zmiana numeru konta	Audyt zmian
Information Disclosure	Wyciek danych	Enpoint API bez zabezpieczeń	Uprawnienia Szyfrowanie
Denial of Service	Niedostępność usługi	Infrastrukturalny Funkcjonalny	Rate limiting IP whitelisting
Elevation of Privilige	Możliwość wykonania nieautoryzowanej akcji	Zmiana uprawnień poprzez SQL Injection	Uprawnienia Walidacja

Globalne modelowanie zagrożeń

- Co budujemy?
- Co może pójść nie tak?
- Plan mitygacji
- Walidacja planu

STRIDE – jak zaaplikować

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of Service	Elevation of Privilige
Proces	X		X		X	
Przepływ	X	X	X	X	X	X
Baza danych		X	X	X	X	
Zewnętrzny obiekt		X		X	X	



Globalne modelowanie zagrożeń

Co budujemy?

Co może pójść nie tak?

Plan mitygacji

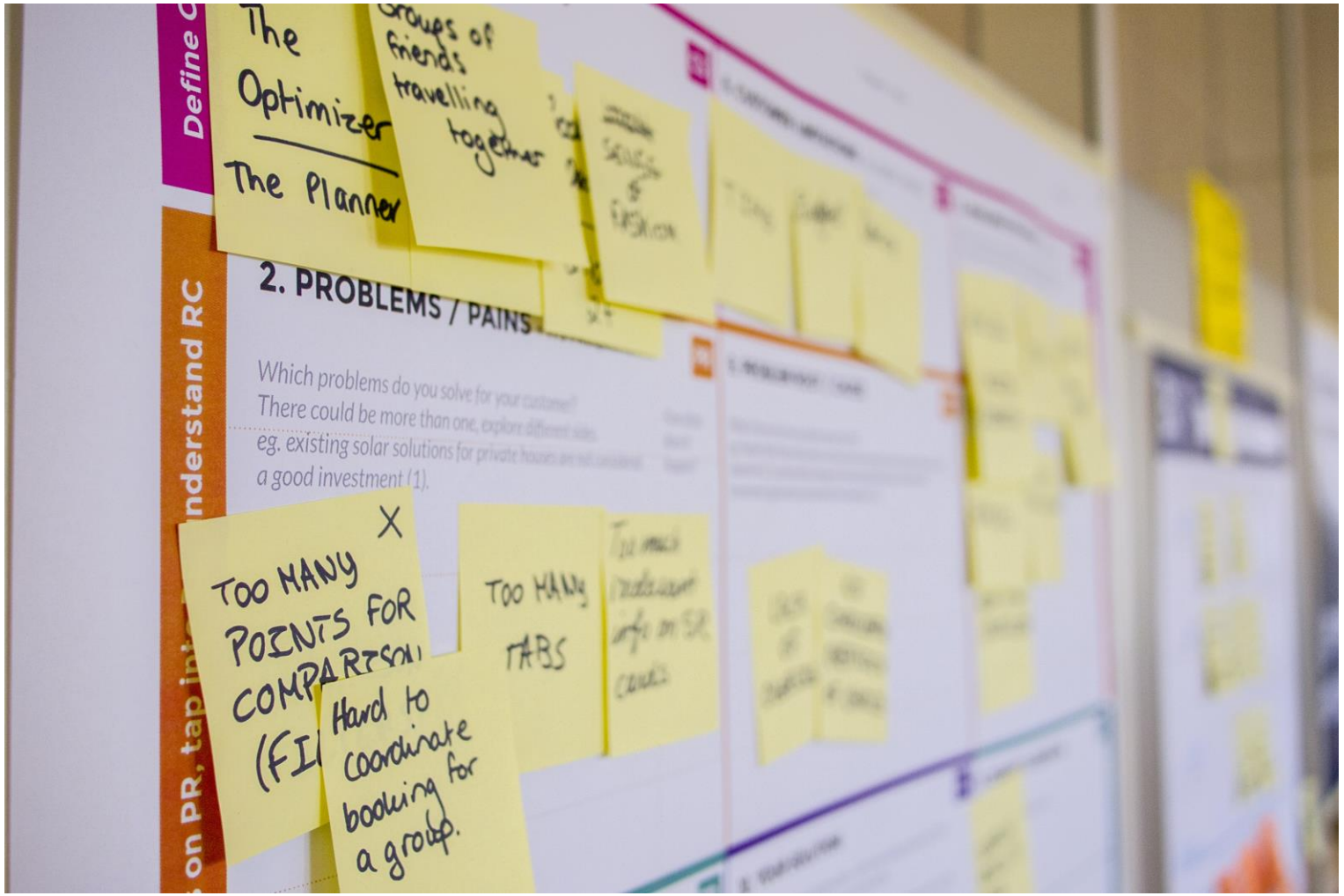
Walidacja planu

- Akceptacja
- Unikanie
- Mitygacja
- Przeniesienie

OWASP Cheatsheets

Globalne modelowanie zagrożeń

- Co budujemy?
- Co może pójść nie tak?
- Plan mitygacji
- Walidacja planu



Globalne modelowanie zagrożeń Narzędzia

- Microsoft Threat Modelling Tool (darmowe)
- OWASP Threat Dragon (darmowe)
- Irius (płatne)
- Inne narzędzia do rysowania diagramów
- Ołówek i długopis (płatne)

Globalne podejście – główne problemy

- Nastawione na pojedynczy element architektury systemu
- Nie analizuje powiązań pomiędzy elementami
- Czasochłonne
- Wymaga sporej wiedzy na start

Iteracyjne modelowanie zagrożeń

CO SPRINT

PODCZAS REFINEMENTU

CAŁY ZESPÓŁ

Iteracyjne modelowanie zagrożeń

- Refinement
- Modelowanie zagrożeń
- Dokumentacja
- Mitygacje
- Zakres zadania

Iteracyjne modelowanie zagrożeń

Refinement

Modelowanie zagrożeń

- **Burza mózgów**
- Pytania STRIDE
- Kwestionariusz bezpieczeństwa

Dokumentacja

Mitygacje

Zakres zadania

Iteracyjne modelowanie zagrożeń

Refinement

Modelowanie zagrożeń

- Burza mózgów
- **Pytania STRIDE**
- Kwestionariusz bezpieczeństwa

Dokumentacja

Mitygacje

Zakres zadania

- Spoofing – Czy ktoś może podszyć się pod kogoś innego?
- Tampering – Czy ktoś może zmodyfikować dane wysyłane/przetwarzane przez aplikację wbrew regułom systemu?
- Repudiation - Czy ktoś może wykonać jakąś akcję bez możliwości udowodnienia mu tego?
- Information disclosure - Czy ktoś może uzyskać dostęp do danych, do których normalnie nie powinien mieć dostępu?
- Denial of Service - Czy ktoś może spowodować niedostępność systemu?
- Elevation of Privilege - Czy ktoś może wykonać akcję wykraczającą poza jego uprawnienia?

Iteracyjne modelowanie zagrożeń

Refinement

Modelowanie zagrożeń

- Burza mózgów
- Pytania STRIDE
- **Kwestionariusz bezpieczeństwa**

Dokumentacja

Mitygacje

Zakres zadania

Jeżeli dotyczy…	…zadaj następujące pytania
Architektura	Czy system produkcyjnie udostępnia publicznie dokumentację (np. do API)?
Backendowa integracja z innymi usługami	W jaki sposób zabezpieczamy komunikację?
	Jakie sekrety są używane z komunikacji?
	Czy użytkownicy mają dostęp do sekretów?
	Czy możemy w wygodny sposób zmienić sekret?
	Czy deweloperzy mają dostęp do produkcyjnych sekretów?
Upload plików	Jak zabezpieczony jest upload?
	Czy walidujemy rozmiar, typ i rozszerzenie pliku?

Iteracyjne modelowanie zagrożeń

Refinement

Modelowanie zagrożeń

Dokumentacja

Mitygacje

Zakres zadania

- Przypadki nadużyć (Abuse Story)
- Przypadki testowe
- Kryteria akceptacji

Iteracyjne modelowanie zagrożeń

Refinement

Modelowanie zagrożeń

Dokumentacja

Mitygacje

Zakres zadania

- Rejestr popularnych zagrożeń i mitygacji
- Rejestr mitygacji z innych systemów

Iteracyjne modelowanie zagrożeń

- Refinement
- Modelowanie zagrożeń
- Dokumentacja
- Mitygacje
- Zakres zadania

- Co w ramach historyjki?
- Co jako osobne zadanie?
- Co propagujemy na inne systemy?

Rekomendacje

Dostosuj sposób modelowania do doświadczenia osób, które biorą w nim udział

- Burza mózgów
- Pytania STRIDE
- Kwestionariusz bezpieczeństwa

Im dalej, tym precyzyjniejsze wskazówki

Jak wdrażać threat modelling w firmie?

- Wybierz odpowiednie podejście
- Wybierz ewangelistów / security champions
- Dostosuj framework do swoich potrzeb
- Zacznij praktykować
- Dostosowuj proces

Zaproszenie i prośba

Jeżeli chcesz wdrożyć modelowanie zagrożeń w swoim zespole/swojej firmie, mogę Ci w tym pomóc.

Napisz do mnie: security@diwebsity.com z dopiskiem w temacie [Threat Modelling]

Dziękuję za uwagę