

Modelowanie Zagrożeń (ang. *threat modeling*)

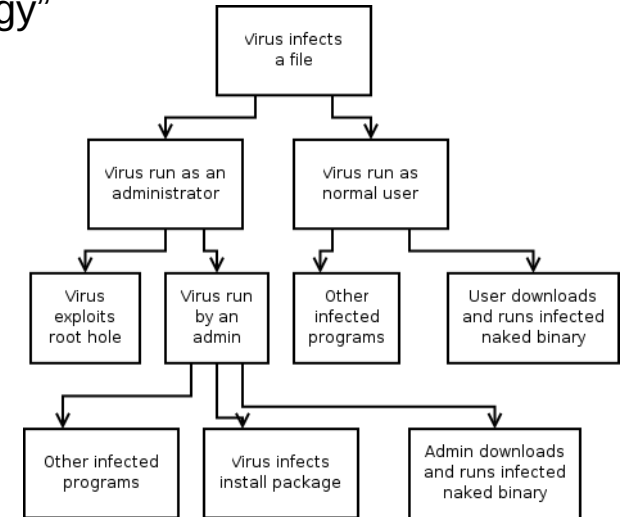
Modelowanie zagrożeń – definicja

- Proces skupiający się na:
 - Identyfikowaniu
 - Priorytetyzacji
 - Enumeracji

.... strukturalnych zagrożeń z punktu widzenia potencjalnego atakującego
- Jest systematyczną analizą profilu atakującego i odpowiada na pytania jakie zasoby mogą być dla niego pożądane
- Identyfikuje wektory ataku i służy do identyfikacji powierzchni ataku

Jak to się zaczęło...

- 1994 Edward Amoroso „Fundamentals of Computer Security Technology”
- koncepcja drzewa zagrożeń bazująca na drzewie decyzyjnym (ang. *threat trees*)
- 1998 Bruce Schneier „Toward a Secure System Engineering Metodology”
- koncepcja drzew ataku (ang. *attack trees*)
- 1999 Microsoft, Loren Kohnfelder i Praerit Grag – metodyka STRIDE
- 2003 CMU – metodyka OCTAVE
- 2005 Mark Nicolett i Amrit Williams (Gartner), koncepcja narzędzi SIEM (security information and event management)
- 2014 Ryan Stillions model DML (ang. Detection Maturity Level), atakujący skupia się na celu stosując TTP (taktyki, techniki, procedury) szacowane na odpowiednich poziomach



SIEM – komponenty i znaczenie

- Agregacja danych
- Wykrywanie korelacji
- Ostrzeżenia i alerty
- Predykcja i trendy (tablica)
- Korelacja z działaniami w innych systemach
- Retencja danych historycznych
- Analiza po zdarzeniu (ang. *forensic*)

Zakres metodyk modelowania zagrożeń

	OCTAVE	Trike	P.A.S.T.A.	STRIDE	VAST
Bezpieczeństwo na etapie projektowania	•	•	•	•	•
Identyfikowanie metod łagodzenia	•	•	•	•	•
Zarządzanie ryzykiem	•	•	•	•	•
Priorytetyzacja środków zaradczych	•	•	•		•
Wymaganie współpracy wszystkich związanych z projektem	•	•			•
Przedstawiana wszystkim w organizacji	•				•
Powtarzana i ciągła		•			•
Automatyzacja modelowania zagrożeń		•			•
Zintegrowana z Agile i DevOps (CI)					•
Zdolna do skalowania na cały model zagrożeń					•

OCTAVE

- OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Metodyka utworzona na CMU (Carnegie Mellon University) w ramach SEI (Software Engineering Institute)
- Bazuje na szacowaniu nie-technicznych ryzyk w ramach audytu organizacji, wpływających na dane wrażliwe
- Określa przepływy danych i zasoby oraz główne ryzyka bezpieczeństwa organizacji.
- Zalety:
 - Dobra publicznie dostępna dokumentacja
 - Łatwe dostosowanie
- Konsekwencje:
 - Stosowana jako wstęp do budowy kultury organizacji w obszarze bezpieczeństwa
 - Bardzo ogólna

TRIKE

- Używa modelu zagrożeń jako narzędzia zarządzania ryzykiem
- Bazuje na „modelu wymagań” jako akceptowalnym poziomie ryzyka z punktu widzenia udziałowca/osoby odpowiedzialnej (ang. *stakeholder*)
- Kompletny model zawiera obliczone poziomy ryzyka z zasobami, rolami, akcjami (sposobami reakcji na ryzyko).
- Zaleta:
 - Modelowanie przepływu danych znanym DFD (zapis, przeniesienie, proces, integracja)
 - Ścisłe odpowiedzi co do ryzyk
 - Otwartoźródłowa: <http://www.octotrike.org/>
- Konsekwencje:
 - Wymaga zaznajomienia się z metodykami analizy i szacowania ryzyka

P.A.S.T.A.

- P.A.S.T.A. - Process for Attack Simulation and Threat Analysis
- Siedem kroków do zbliżenia wymagań bezpieczeństwa biznesu z aspektami technicznymi
- Cel to zbudowanie dynamicznego modelu identyfikacji, określania i szacowania ryzyk bezpieczeństwa
- Przedstawia zagadnienia bezpieczeństwa z punktu widzenia atakującego
- Zaleta:
 - Systematyzuje wiele pojęć obecnych w innych modelach
 - Uzupełnia modele o elementy modelu symulacji ataku jako ostatecznego testu prawdziwości założeń
- Konsekwencje:
 - Nie adresuje wszystkich zagadnień związanych z bezpieczeństwem

STRIDE

- STRIDE – Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
- Adresuje wymagania dyrektywy Trustworthy Computing (styczeń 2002) w zakresie CIA (Confidentiality, Integrity, Availability)
- Wspierane przez narzędzie Microsoft TMT

VAST

- VAST - Visual, Agile, and Simple Threat
- Zakłada skalowanie procedur i narzędzi do rozmiaru organizacji i wyzwań
- Adresuje dwie warstwy:
 - Aplikacyjny model zagrożeń – poprzez analizę PFD (ang. *process flow diagrams*)
 - Operacyjny model zagrożeń – aspekt procesów i procedur
- Osadza działania we współczesnym DevOps adresując wymagania uczestników projektu
- Zalety:
 - Skalowalność i elastyczność
 - Odniesienie do współczesnych praktyk wytwarzania produktów związanych z oprogramowaniem
- Konsekwencje:
 - Wymaga świadomego dostosowania do całości przedsiębiorstwa
 - Dotyka aspektów organizacyjnych i biznesowych