Analiza dostępnych metod oceny krytyczności podatności metodą SWOT

CVSS

Zalety	Wady
Mocne strony: • Powszechnie przyjęty i uznany standard. • Zapewnia kompleksowy system punktacji z podstawowymi, czasowymi i środowiskowymi wskaźnikami. • Oferuje znormalizowany sposób informowania o stopniu podatności na zagrożenia.	**Słabe strony:** • Złożoność może utrudniać zrozumienie i zastosowanie tego standardu przez początkujących użytkowników. • Niektóre wskaźniki mogą być subiektywne, co prowadzi do niespójnej punktacji. • Nie zapewnia bezpośredniego mechanizmu ustalania priorytetów.
Szanse: • Potencjał do dalszego rozwoju ze względu na popularność standardu. • Integracja z innymi narzędziami i platformami może zwiększyć jego użyteczność i automatyzację.	**Zagrożenia:** • Subiektywna interpretacja wskaźników może prowadzić do niespójnej punktacji.

DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability)

Zalety	Wady
Mocne strony: • Prosty i intuicyjny model. • Koncentruje się na kluczowych czynnikach wpływających na krytyczność podatności. • Zapewnia numeryczny system oceny podatności na zagrożenia.	**Słabe strony:** • Subiektywna punktacja może prowadzić do niespójności. • Nie uwzględnia czynników zewnętrznych ani kontekstu organizacyjnego. • Równa waga parametrów. • Może nie obejmować wszystkich istotnych aspektów krytyczności podatności.
Szanse: • Szkolenie i wytyczne mogą poprawić spójność punktacji i interpretacji. • Modyfikacje modelu mogą uwzględniać ograniczenia i obejmować dodatkowe czynniki. • Ze względu na prostotę modelu może on być wykorzystywany w celu szkolenia personelu w zakresie podstaw oceny krytyczności.	**Zagrożenia:** • Subiektywna ocena może prowadzić do niespójności i stronniczości. • Model, który obejmuje tylko 5 parametrów z równą wagą może nie uwzględniać wszystkich aspektów krytyczności podatności i niewłaściwie ocenić krytyczność.

PASTA (Process for Attack Simulation and Threat Analysis)

Zalety	Wady
Mocne strony: • Kompleksowe i ustrukturyzowane podejście do oceny ryzyka. • Uwzględnia kontekst organizacyjny i zasoby wraz z obszarami ataku. • Pozwala na definiowanie parametrów według potrzeb organizacji.	**Słabe strony:** • Tworzenie modelu jest unikalne dla każdej organizacji, więc zbudowanie tak dokładnego modelu zajmuje dużo czasu. • Wymaga wysokiego poziomu wiedzy na temat potrzeb i struktury organizacji w celu prawidłowego zbudowania modelu. • Może nie nadawać się do szybkiej oceny podatności na zagrożenia.
Szanse: • Przy dobrze wyszkolonym personelu metoda ta może być jedną z najdokładniejszych i najbardziej odpowiednich dla organizacji o specjalnych potrzebach. • Automatyzacja i wsparcie narzędziowe mogą usprawnić proces i zmniejszyć nakład pracy.	**Zagrożenia:** • Czas i poziom wiedzy wymagany do budowy nie jest odpowiedni dla małych organizacji. • Ze względu na złożoność konstrukcji, przy niskim poziomie kompetencji możliwe jest zbudowanie nieprawidłowego modelu, który nie odzwierciedla rzeczywistego poziomu zagrożenia, ze wszystkimi możliwymi konsekwencjami.

STRIDE

Zalety	Wady
Mocne strony: • Zapewnia jasną i uporządkowaną kategoryzację zagrożeń. • Identyfikuje wspólne luki w różnych systemach.	**Słabe strony:** • Koncentruje się głównie na identyfikacji zagrożeń, a nie na krytyczności podatności. • Nie zapewnia bezpośredniego mechanizmu punktacji do ustalania priorytetów. • Może wymagać dodatkowych metod kompleksowej oceny podatności.
Szanse: • Integracja z metodami uzupełniającymi może zapewnić bardziej kompleksową ocenę podatności. • Ciągłe aktualizacje i rozszerzanie kategorii zagrożeń może zwiększyć zastosowanie modelu.	**Zagrożenia:** • Ograniczony nacisk na krytyczność podatności, głównie podkreślając identyfikację zagrożeń. • Brak bezpośredniego mechanizmu punktacji może utrudniać ustalanie priorytetów.

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

Zalety	Wady
Mocne strony: • Koncentruje się na kontekście organizacyjnym i krytycznych zasobach. • Uwzględnia zarówno techniczne, jak i nietechniczne słabe punkty. • Zapewnia systematyczne podejście do oceny ryzyka.	**Słabe strony:** • Wdrożenie wymaga znacznego nakładu czasu i zasobów. • W dużym stopniu opiera się na wiedzy i doświadczeniu organizacyjnym. • Może nie być odpowiedni dla mniejszych organizacji lub ograniczonych ocen.
Szanse: • Uproszczenie i dostosowanie metodologii mogą uczynić ją bardziej dostępną dla szerszego grona organizacji. • Integracja z systemami zarządzania ryzykiem może wzmocnić proces oceny. • Przy odpowiednio wykształconym personelu może być jedną z najlepszych metod dla oceniania krytyczności podatności.	**Zagrożenia:** • Czas i poziom wiedzy wymagany do budowy nie jest odpowiedni dla małych organizacji. • Ze względu na złożoność konstrukcji, przy niskim poziomie kompetencji możliwe jest zbudowanie nieprawidłowego modelu, który nie odzwierciedla rzeczywistego poziomu zagrożenia, ze wszystkimi możliwymi konsekwencjami.

TRIKE (Targeted Risk and Impact Analysis)

Zalety	Wady
Mocne strony: • Zapewnia systematyczne podejście do analizy i priorytetyzacji zagrożeń bezpieczeństwa. • Uwzględnia zarówno techniczny, jak i biznesowy wpływ luk w zabezpieczeniach. • Wspiera podejmowanie decyzji poprzez dostarczanie ocen ryzyka i rekomendacji, które można podjąć.	**Słabe strony:** • Wymaga specjalistycznej wiedzy i znajomości metodologii analizy ryzyka. • Wdrożenie wymaga znacznego nakładu czasu i zasobów • Dokumentacja i wskazówki dotyczące korzystania z TRIKE mogą być ograniczone
Szanse: • Opracowanie przyjaznych dla użytkownika narzędzi i frameworków może uprościć przyjęcie i zastosowanie TRIKE. • Integracja z systemami zarządzania podatnościami może usprawnić proces oceny ryzyka.	**Zagrożenia:** • Czas i poziom wiedzy wymagany do budowy nie jest odpowiedni dla małych organizacji. • Brak ustandaryzowanej implementacji może prowadzić do niespójnych wyników.

LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness)

Zalety	Wady
Mocne strony: • Oferuje ustrukturyzowane podejście do oceny zagrożeń prywatności związanych z systemami informatycznymi. • Koncentruje się na kluczowych atrybutach prywatności i ich wpływie na system. • Zapewnia systematyczny sposób identyfikacji i priorytetyzacji słabych punktów prywatności.	**Słabe strony:** • Zaprojektowany głównie do oceny ryzyka prywatności, może nie obejmować innych aspektów bezpieczeństwa. • Subiektywna interpretacja atrybutów może wprowadzać niespójności w punktacji. • Ograniczona dostępność kompleksowych wskazówek i dokumentacji.
Szanse: • Opracowanie najlepszych praktyk branżowych i studiów przypadku może zwiększyć użyteczność i skuteczność systemu. • Implementacja z innymi systemami może zwiększyć użyteczność.	**Zagrożenia:** • Ograniczona adopcja poza domeną prywatności może ograniczyć jej szersze zastosowanie. • Brak ustandaryzowanej implementacji może prowadzić do niespójnych wyników.

VAST (Visual, Agile, and Simple Threat modeling)

Zalety	Wady
Mocne strony: • Zapewnia uproszczone i wizualne podejście do modelowania zagrożeń. • Kładzie nacisk na współpracę i zwinność w procesie modelowania zagrożeń. • Oferuje elastyczność umożliwiającą dostosowanie do różnych metodologii rozwoju i projektów	**Słabe strony:** • Może nie zapewniać takiego samego poziomu dogłębności i pokrycia, jak bardziej tradycyjne, wyczerpujące podejścia do modelowania zagrożeń. • Może wymagać dodatkowych narzędzi lub frameworków do kompleksowej oceny podatności.
Szanse: • Rozwój narzędzi wspierających i frameworków może zwiększyć użyteczność i wydajność VAST.	**Zagrożenia:** • Uproszczenie procesu może skutkować przeoczeniem krytycznych zagrożeń i podatności.