WNIOSEK O PORTFOLIO:

Koncepcja metodyki oceny ryzyka bezpieczeństwa systemów informatycznych.

Autorzy: Paweł Skrzyński

Centrum Inteligentnych Systemów Informatycznych Akademia Górniczo-Hutnicza im. Stanisława Staszica al. Mickiewicza 30, 30-059 Kraków
budynek C-2 pokój 426 tel.: 12 617 44 53 www.isi.agh.edu.pl **isi@agh.edu.pl**

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Koncepcja metodyki oceny ryzyka bezpieczeństwa systemów informatycznych.

1. Opis merytoryczny.

a. cel naukowy – jaki problem wnioskodawca podejmuje się rozwiązać, co jest jego istotą, co uzasadnia podjęcie tego problemu, jakie przesłanki skłaniają wnioskodawcę do podjęcia proponowanego tematu.

Celem projektu jest opracowanie lekkiej metodyki, która pozwali na na ocenę ryzyka dla systemów informatycznych pod względem bezpieczeństwa ze szczególnym uwzględnieniem złożonych systemów informatycznych. Jako "lekka" rozumiana jest metodyka, której zastosowanie nie wymaga ponoszenia dużych nakładów (zarówno czasowych jak i finansowych) oraz dostarczająca szybko wiarygodnych wyników.

Temat jest ważny ze względu na następujące czynniki:
a) Bezpieczeństwo jest kluczowym wymaganiem stawianym w stosunku do wielu systemów. Zwłaszcza dotyczy to systemów przetwarzających wrażliwe dane i korzystających z publicznej infrastruktury sieciowej.
b) Klasyczne metodyki oceny jakości zabezpieczeń i ryzyka ich naruszenia są ciężkie i nie zawsze możliwe do zastosowania: np. w CRAMM czy NIST wymagane jest finansowe oszacowanie strat płynących z różnych czynników ryzyka oraz oszacowanie prawdopodobieństwa ich wystąpienia.
c) Przy zastosowaniu podejścia klasycznego nie jest możliwa wczesna ocena ryzyka (przed pełną integracją i wdrożeniem). Trudno jest np.: oceniać potencjalne straty dla systemu w trakcie implementacji i wdrożenia.
d) Współczesne zwinne praktyki implementacji oprogramowania pomijają ocenę ryzyka lub redukują ją do sprawdzenia zgodności rozwiązań z listą dobrych praktyk. Praktyki te mogą być niezmieniane przez długi czas, mechanicznie stosowane do kolejnych systemów. W dłuższej perspektywie prowadzi to do zwiększenia podatności na nowe zagrożenia.

b. istniejący stan wiedzy w zakresie tematu badań - jaki oryginalny wkład wniesie rozwiązanie postawionego problemu do dorobku danej dyscypliny, czy jest to problem nowy czy kontynuowany,

Zgodnie z definicją zaproponowaną przez Guttmana i Robacka (1995) bezpieczeństwo systemów informatycznych obejmuje ochronę integralności danych i funkcji, ich dostępność, autentyczność oraz poufność.
Powszechnie stosowanym podejściem do oceny ryzyka dla systemów o niekrytycznych wymaganiach jest metryka ALE (Annual Loss Expectancy). Definiuje ona ryzyko jako iloczyn straty wyrażonej w jednostkach walutowych oraz prawdopodobieństwa wystąpienia zagrożenia. W niektórych modelach może być takze brana pod uwagę podatność na zagrożenie. Opisane

podejście jest podstawą wszystkich ciężkich metod oceny ryzyka i zarządzania ryzykiem (CRAMM, NIST, SABSA, standardy zebrane w zestawieniu ENISA). Ocena ryzyka zgodnie z wymienionymi standardami jest bardzo czasochłona i obarczona jest dużą niepewnością.
Ze względu na nacisk na produktywność i redukcję czasu wdrożenia systemów IT, wiele organizacji odeszło od ciężkich standardów oceny ryzyka. Stosowane rozwiązania obejmują metody oparte na wartościowaniu aktywów (stosowane są zabezpieczenia adekwatne do ich wartości), analizy scenariuszowe ataków oraz dobre praktyki.

Zgodnie z postawioną diagnozą istnieje luka pomiędzy ciężkimi metodami oceny ryzyka i panującymi praktykami: nie prowadzi się oceny zagrożeń dla poszczególnych systemów (ponieważ jest to zbyt kosztowne), natomiast wybór zastosowanych zabezpieczeń nie opiera się na modelach ryzyka, ale predefiniowanych listach przygotowanych zgodnie z regułami najlepszych praktyk.

Oryginalnym wkładem projektu jest propozycja lekkiej metodyki oceny bezpieczeństwa dla różnych klas systemów informatycznych. W zamierzeniu metoda ta ma integrować współczesne rozwiązania (dobre praktyki, wartościowanie aktywów), obejmować techniki grupowej oceny przez ekspertów, wykorzystywać artefakty cyklu życia oprogramowania oraz stosować podejście do agregacji ryzyka wykorzystujące wnioskowanie przybliżone, a zwłaszcza Rozmyte Mapy Kognitywne (ang. Fuzzy Cognitive Maps).

Szersze omówienie istniejącego stanu wiedzy znajduje się w publikacji:

A new lightweight method for security risk assessment based on fuzzy cognitive maps, Piotr SZWED, Paweł SKRZYŃSKI, International Journal of Applied Mathematics and Computer Science ; ISSN 1641-876X. — 2014 vol. 24 no. 1, s. 213–225.

1. CRAMM: http://www.cramm.com/
2. NIST 800-30, Guide for conducting risk assessments, nist sp - 800-30rev1, Nist Special Publication (September): 85.
3. Standardy Enisa: http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html
4. http://www.sabsa-institute.org/the-sabsa-method

c. metodyka badań – co stanowi podstawę naukowego warsztatu wnioskodawcy i jak zamierza rozwiązać postawiony problem, jakie urządzenia (aparatura) zostaną wykorzystane w badaniach,

Proponowane we wniosku podejście w zamierzeniu ma wykorzystać modele i techniki stosowane w inżynierii oprogramowania, modelowania biznesowego, opisy semantyczne w postaci ontologii oraz wnioskowanie przybliżone.

Planowane cechy metodyki:

- Wykorzystanie rezultatów cyklu rozwoju oprogramowania (w tym modeli architektury, zidentyfikowanych procesów i ról) do identyfikacji aktywów
- Wykorzystanie podczas analiz informacji o najlepszych praktykach dotyczących zabezpieczeń stosowanych w danej dziedzinie zastosowań
- Wykorzystanie w ocenie wiedzy ekspertów, technik głosowania i usuwania rozbieżności
- Zastosowanie modeli i technik wnioskowania przybliżonego (w tym rozmytych map kognitywnych) do modelowania i agregacji ryzyka.
- Formalizacja metodyki obejmująca: klasy opisywanych obiektów i ich powiązania (aktywa, zagrożenia, zabezpieczenia), opis procesowy czynności wykonywanych podczas oceny ryzyka oraz artefakty powstające w poszczególnych etapach.
- Możliwość wielokrotnego użycia rezultatów analiz: listy najlepszych praktyk, klas aktywów, taksonomii zagrożeń dla systemów tej samej klasy

d. co będzie wymiernym, udokumentowanym efektem podjętego problemu – nowe patenty „know-how", nowe metody, urządzenia, implikacje, konsekwencje, walory.

Wymiernym efektem projektu będzie opracowanie nowej metodyki oceny bezpieczeństwa systemów informatycznych. Rezultaty szczegółowe obejmowały będą:

- Analizę najlepszych praktyk dotyczących zabezpieczeń
- Ogólną hierarchię zagrożeń wraz z egzemplifikacjami odnoszącymi się do wybranych klas systemów
- Formalny metamodel opisujący przetwarzane informacje oraz wytwarzane artefakty
- Przykłady zastosowań metodyki podczas oceny ryzyka dla konkretnych systemów
- Publikacje

2. Charakterystyka i typ potencjalnych nabywców:

a. partnerzy z przemysłu, biznesu potencjalnie zainteresowani rozwiązaniem,

Można wyróżnić kilka typów nabywców:

- Nabywcy zainteresowani usługą polegającą na ocenie ryzyka bezpieczęństwa dla wybranych instancji systemów. Dotyczy to dostawców złożonych systemów

teleinformatycznych oraz instytucje wdrażające systemy, w których bezpieczeństwo odgrywa kluczową rolę.

- Dostawcy oferujący wdrożenie produktu o podwyższonych wymaganiach dotyczących bezpieczeństwa. Ocena ryzyka powinna być przeprowadzona wielokrotnie dla różnych instancji systemu z wielokrotnym wykorzystaniem modelu ryzyka (aktywów, zagrożeń, podatności). Tym samym uzasadniona jest implementacja narzędzia wspierającego tę ocenę.
- Nabywcy zainteresowani komercjalizacją metodyki i budową dedykowanego narzedzia informatycznego.
- Podmioty komercyjne zainteresowane rozwiązaniem: 1App SA, Getin Noble Bank SA, WOW Sp. z o.o..

b. jednostki samorządowe i instytucje potencjalnie zainteresowane rozwiązaniem,

Wszelkie instytucje dokonujące wdrożeń systemów teleinformatycznych, gdzie bezpieczeństwo jest istotnym elementem.

c. obszary przemysłu, biznesu, w których można zastosować rozwiązanie.

Wszelkie instytucje dokonujące wdrożeń systemów teleinformatycznych, gdzie bezpieczeństwo jest istotnym elementem. W szczególności dotyczy to systemów, które powinna cechować niezawodność,duża dostępność oraz wysoki poziom bezpieczeństwa dla przetwarzanych danych poufnych. Jako szczególne przykłady można wskazać instytucje finansowe, ubezpieczeniowe, jednostki medyczne, czy firmy energetyczne.

3. Opis istniejących materiałów promocyjnych, które mogą być wykorzystane do promocji np: projekty, zdjęcia, szkice, wizualizacje.

Dokumenty opisujące metodykę, prezentacje obrazujące jej zastosowanie, przykładowe wyniki z aplikacji metodyki na rzeczywistych systemach. Materiały promocyjne powinny być jednak adresowane dla konkretnej branży.

4. Potencjalni rozmówcy (autorytety w dziedzinie), wywiady z którymi pozwolą podnieść jakość rozwiązania.

dr maj. Bartosz Jasiul, Wojskowy Instytut Łączności

5. Kierunki potencjalnego zastosowania projektu.

1. Wdrożenia złożonych systemów informatycznych.
2. Audyty bezpieczeństwa istniejących systemów.

6. Opis silnych i słabych strony projektu.

Silne strony:
1. Łatwość i szybkość wykorzystania wyników
2. Niskie koszty zastosowania.

Słabe:

- wyniki uzależnione od wiedzy dziedzinowej ekspertów zaangażowanych w proces
- brak narzędzi wspomagających przeprowadzenie procesu ewaluacji ryzyka z wykorzystaniem proponowanej metodyki

7. Wskazania czynników ryzyka.

Czynnik	Ryzyko	Komentarz
Brak dostępu do specyfikacji systemu, opisów architektury i funkcji.	średnie	Problem dotyczy systemów rozwijanych zgodnie ze zwinnym podejściem. W tym przypadku konieczne jest zebranie informacji w trakcie wywiadów z zepsołem.
Problem z zebraniem informacji od ekspertów, architektów systemu i zespołu wykonawczego	średnie	Planowana jest zastosowanie technik burzy mózgów
Stronniczość ocen, odpowiedzi zmierzające do zmniejszenia ocenianego ryzyka	duże	Jest to znany problem wszystkich metod.
Brak danych porównawczych pozwalających na kalibrację ryzyka	średnie	Jest to również problem większości metod (benchmarking). Przy braku danych historycznych kalibracja jest możliwa przez zebranie informacji o dobrymi praktykach.

Opór decydentów przed zastosowaniem wnioskowania przybliżonego	średnie	
Brak narzędzi wspierających zastosowanie metodyki	małe	
Brak możliwości porównania rezultatów z metodykami uznanmi za referencyjne	duże	Metodyki referencyjne sa ciężkę i koszt przeprowadzenia oceny nawet dla średniej klasy systemów jest duży