STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Dariusz ROGOWSKI
Instytut Systemów Sterowania w Chorzowie

METODYKA OCENY ZABEZPIECZEŃ TELEINFORMATYCZNYCH[1]

Streszczenie. Referat przedstawia metodykę prowadzenia oceny zabezpieczeń teleinformatycznych, która została opracowana w oparciu o rodzinę międzynarodowych norm pt. „Wspólne Kryteria do Oceny Zabezpieczeń Teleinformatycznych" (ISO/IEC 15408). W referacie opisano główne zasady, założenia oraz model ogólny procesu prowadzenia oceny zabezpieczeń, zmierzającego do wydania końcowego werdyktu dla produktu. Omówiono także przykład oceny fragmentu Zadania Zabezpieczeń aplikacji SecOffice przeznaczonej do szyfrowania i podpisywania dokumentów elektronicznych.

Słowa kluczowe: metodyka, ocena, jednostka oceny, komponent, Wspólne Kryteria, Zadanie Zabezpieczeń, Profil Zabezpieczeń, Przedmiot Oceny, SecOffice.

EVALUATION METHODOLOGY FOR IT SECURITY

Summary. The paper presents methodology of evaluation process conducting according to the family of international standards Common Criteria for IT Security Evaluation (ISO/IEC 15408). The paper describes the main principles, assumptions and general model of the IT security evaluation process, leading to the product's final verdict. The paper presents an example of the Security Target evaluation of SecOffice application used to digital signature and encryption of electronic documents.

Keywords: methodology, evaluation, work unit, component, Common Criteria, Security Target, Protection Profile, Target of Evaluation, SecOffice.

[1] Praca została wykonana w ramach projektu celowego KBN nr 6.T11.073.2001C/5689.

1. Wprowadzenie

Wielu odbiorców produktów teleinformatycznych nie posiada odpowiedniej wiedzy, doświadczenia lub zasobów koniecznych, aby osądzić, czy ich zaufanie do zabezpieczeń produktów lub systemów teleinformatycznych jest uzasadnione, a jednocześnie nie chcą oni opierać się jedynie na deklaracjach konstruktorów. Odbiorcy mogą w związku z tym zdecydować się na zwiększenie zaufania do zabezpieczeń produktu lub systemu teleinformatycznego poprzez dokonanie analizy jego zabezpieczeń prowadzonej według jasno określonych zasad umieszczonych w rodzinie międzynarodowych norm pt. „Wspólne Kryteria do Oceny Zabezpieczeń Teleinformatycznych" [1-5], które od 1999 roku uzyskały status standardu ISO/IEC 15408 i powstały wysiłkiem międzynarodowym z ujednolicenia standardów lokalnych. Dokumentem uzupełniającym normę jest Metodyka Ewaluacji *(ang. CEM – Common Evaluation Methodology)* [4, 5]. Opisuje ona przebieg procesu oceny i sposób wydawania werdyktów.

Prowadzenie oceny zabezpieczeń jest procesem skomplikowanym, trudnym, wymagającym od oceniającego eksperckiej wiedzy z dziedziny Wspólnych Kryteriów *(ang. CC – Common Criteria)*, dlatego też prace prowadzone w ramach Projektu Celowego KBN doprowadziły m.in. do powstania metodyki oceny zabezpieczeń [10], która ma w wydatny sposób ułatwić pracę oceniającym. Ten swoisty przewodnik ma być wyjściowym dokumentem umożliwiającym utworzenie algorytmów i formalizację zapisów poszczególnych etapów całego ciągu procesu oceny.

W niniejszym referacie skupiono się na całościowym zaprezentowaniu procesu oceny zabezpieczeń, jego poszczególnych etapów, głównych zasad i założeń. Przedstawiono także przykład oceny wybranego fragmentu Zadania Zabezpieczeń *(ang. ST – Security Target)* dla oprogramowania kryptograficznego SecOffice firmy Sotel. Omawiany fragment dokumentu ST dotyczy opisu otoczenia zabezpieczeń aplikacji SecOffice, którego ocenę można przeprowadzić za pomocą jednego komponentu uzasadniającego zaufanie do zabezpieczeń *(ang. security assurance component)*.

2. Główne zasady i założenia prowadzenia ocen

Za rozpoczęcie procesu oceny produktu teleinformatycznego odpowiedzialny jest zleceniodawca *(ang. sponsor)*, którym może być jednostka organizacyjna zamawiająca ocenę, konstruktor lub klient. Nad poprawnością działań oceniających czuwa nadzorujący *(ang. overseer)*, którym jest najczęściej odpowiednia jednostka certyfikująca.

Prawidłowe i wiarygodne wyniki działań oceniających będzie można uzyskać tylko wtedy, gdy zarówno działania oceniającego, jak i dokumentacja, która będzie ich wynikiem, spełnią kilka podstawowych zasad, które zostały określone w części 1 CEM [4]:

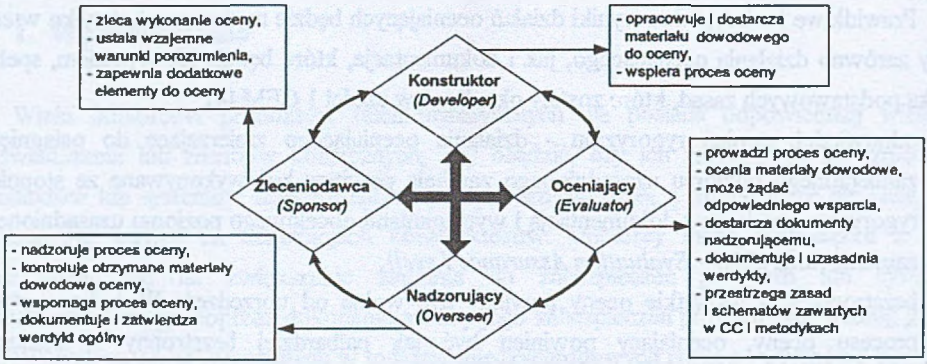
- odpowiedni stopień rygoryzmu - działania oceniającego zmierzające do osiągnięcia zamierzonego poziomu uzasadnionego zaufania powinny być wykonywane ze stopniem rygoryzmu zgodnym z dokumentacją i wymaganiami docelowego poziomu uzasadnionego zaufania *(ang. EAL – Evaluation Assurance Level)*,
- bezstronność - wszystkie oceny powinny być wolne od uprzedzeń. W żadnym etapie procesu oceny, oceniający powinien być jak najbardziej bezstronny w stosunku do ocenianego Przedmiotu Oceny *(ang. Target of Evaluation)* lub Profilu Zabezpieczeń *(ang. Protection Profile)*,
- obiektywność - oceny powinny być uzyskiwane z minimalnym subiektywnym osądem,
- powtarzalność i odtwarzalność wyników - powtórzona ocena tego samego produktu z tymi samymi wymaganiami oraz dowodami powinna dostarczać tych samych wyników,
- przedstawianie wyników - wyniki oceny powinny być kompletne i technicznie poprawne.

Podstawowe zasady poprawnego przeprowadzania ocen wywodzą się z kolei z konieczności spełnienia założeń, odnoszących się do środowiska oceny i wszystkich działań z nią związanych:

- efektywność kosztów - wartość oceny powinna kompensować czas, zasoby i finanse zużywane w ciągu całego procesu oceny,
- przyszły rozwój metodologii - wpływ zmian czynników środowiskowych i technicznych na proces oceny powinien być odzwierciedlony w metodologii oceny, która musi brać pod uwagę otoczenie zabezpieczeń i musi być stosowalna w nowych, rozwijających się technologiach,
- możliwość ponownego użycia - procesy ocen powinny umożliwiać efektywne wykorzystanie poprzednich wyników ocen.

3. Ogólny model oceny

W ogólnym modelu postępowania należy jasno określić poszczególne zadania zleceniodawcy, konstruktora, oceniającego oraz nadzorującego, za które ponoszą odpowiedzialność w kolejnych etapach oceny opisanych w metodyce (rys. 1).



Rys. 1. Odpowiedzialność i związki pomiędzy stronami procesu oceny
Fig. 1. Responsibility and relationships of the evaluation process parties

Pierwszy etap otwierający proces oceny nazywa się **przygotowaniem** *(ang. Preparation)* [4], [10]. W tej fazie zleceniodawca zwraca się do stosownej organizacji oceniającej w celu rozpoczęcia oceny PP, ST lub TOE. Zleceniodawca dostarcza oceniającemu odpowiednich dokumentów (PP lub ST) i innych materiałów dowodowych. Oceniający wykonuje analizę wykonalności w celu wyznaczenia prawdopodobieństwa pomyślnego zakończenia procesu oceny. Zleceniodawca lub konstruktor mają obowiązek dostarczyć oceniającemu odpowiedniego podzbioru elementów do ceny, także w formie wstępnych projektów *(ang. Draft Projects)*.

Etap **prowadzenia** *(ang. Conduct)* oceny jest podstawową częścią całego procesu. W jego trakcie oceniający przegląda otrzymane od zleceniodawcy elementy do oceny i wykonuje działania wymagane przez odpowiednie kryteria uzasadniające zaufanie do zabezpieczeń produktu. W trakcie oceny oceniający sporządza raporty z uwagami wstępnymi *(ang. OR - Observation Reports)*, na podstawie których może żądać od nadzorującego wyjaśnienia zastosowania poszczególnych wymagań. Oceniający sporządza także raport techniczny oceny *(ang. ETR - Evaluation Technical Report)*, który zawiera werdykt ogólny wraz z jego uzasadnieniem.

W fazie wyciągania **wniosków** *(ang. Conclusion)* oceniający dostarcza dokumentu ETR nadzorującemu, który przegląda i analizuje raport techniczny w celu oceny jego zgodności z CC oraz CEM. Nadzorujący wydaje werdykt końcowy *(ang. Oversight Verdict)*, zgadzając się bądź nie z werdyktem ogólnym zawartym w ETR oraz przygotowuje raport podsumowujący ocenę *(ang. ESR - Evaluation Summary Report)*.

Dokument ETR traktowany jest jako główny punkt wyjścia dla informacji zawartych w raporcie ESR, który ostatecznie zostaje przekazany do organu nadzorującego ocenę.

4. Główne zadania procesu oceny

Proces oceny PP lub TOE (włącznie z ST) składa się z dwóch podstawowych zadań oceniającego: zadania wejściowego i zadania wyjściowego, które określają sposoby zarządzania dowodami oceny i generowania raportów.

Wyjścia oceny zawarte są w ETR, rzadziej w OR. Zakres komponentów oceny, w przypadku oceny TOE, zmienia się w zależności od wymagań uzasadniających zaufanie opisanych w części 3 CC [3].

Celem **zadania wejściowego** jest zapewnienie oceniającemu właściwych dowodów niezbędnych dla prowadzenia procesu oceny i odpowiedniej ich ochrony. Odpowiedzialność za dostarczenie wszystkich wymaganych dowodów leży po stronie zleceniodawcy. Jednakże większość z nich jest opracowywana i udostępniana przez konstruktora w imieniu zleceniodawcy. Często oceniający wspólnie ze zleceniodawcą tworzą wykaz wymaganych elementów do oceny.

Oceniający powinien posługiwać się wyłącznie ostateczną, formalną wersją materiałów dowodowych, ale dopuszcza się także stosowanie dowodów w formie wstępnych projektów, które pozwalają na wydanie wcześniejszej, nieformalnej oceny. Takie dokumenty wykorzystywane są w sytuacjach, w których ocena TOE prowadzona jest w trakcie jego projektowania, co pozwala projektantowi na poprawienie błędów i uzupełnienie braków zauważonych przez oceniającego lub zapewnienie materiałów dla oceny zabezpieczeń nie uwzględnionych w istniejącej dokumentacji (np. ma to miejsce w przypadku TOE, który od początku nie był projektowany zgodnie z wymaganiami CC).

Celem **zadania wyjściowego** jest sporządzenie przez oceniającego raportu z uwagami wstępnymi (OR) oraz raportu technicznego oceny (ETR). CEM jasno określa niezbędne minimum informacji, które muszą zawierać raporty i jednocześnie nakłada wymóg braku sprzeczności w raportowaniu wyników ocen, który umożliwia spełnienie podstawowej zasady powtarzalności i odtwarzalności rezultatów.

Każdy raport powinien zawierać identyfikator ocenianego PP, ST lub TOE oraz wymieniać wszystkie zadania i działania, w trakcie których powstały krytyczne uwagi. Raport wskazuje instytucję odpowiedzialną za rozwiązanie poszczególnych problemów, których ciężar musi być wcześniej określony (np. negatywny werdykt, wstrzymanie procesu oceny) oraz opracowuje harmonogram działań naprawczych wraz z oszacowaniem wpływu ich ewentualnego niepowodzenia na dalszy bieg oceny.

Dokument ETR zawiera techniczne uzasadnienie werdyktów oceny. Raport pomaga nadzorującemu w wydaniu werdyktu końcowego.

5. Formalna notacja własności bezpieczeństwa

Wspólne Kryteria określają formalny aparat, pozwalający na wyrażanie funkcjonalności zabezpieczeń, mierzalnej wiarygodności zabezpieczeń, a przy tym zapewniający jednorodność i powtarzalność ocen. Podstawowym modułem do tworzenia specyfikacji jest komponent. Dla danego zbioru komponentów funkcjonalnych poziom uzasadnionego zaufania EAL może się różnić znacząco i zależy głównie od rygoryzmu zaaplikowanego przy tworzeniu TOE. Część trzecia CC zawiera katalog komponentów uzasadniających zaufanie oraz wyrażoną za ich pomocą predefiniowaną skalę pomiarową w postaci poziomów uzasadnionego zaufania od EAL1 do EAL7. Komponenty uzasadniające zaufanie wyrażają elementarne rygory, które twórca uwzględnia przy opracowaniu TOE, a oceniający podczas jego oceny. Produkty o tej samej funkcjonalności bezpieczeństwa (ten sam zbiór komponentów funkcjonalnych) mogą powstawać w mniej lub bardziej rygorystyczny sposób, więc uzasadnione zaufanie do nich, wyrażone w skali EAL1 do EAL7, może być różne.

Przyjęto trójpoziomową, hierarchiczną strukturę katalogów: klasa – rodzina – komponent. Klasa obejmuje grupę wymagań z pewnego wspólnego obszaru, np. grupy celów zabezpieczeń. Zawiera ona rodziny ukierunkowane na realizację wybranych celów, różniące się jednak rygoryzmem. Rodzina składa się z jednego lub kilku komponentów. Dodatkowo, komponent składa się z elementów, które stanowią najniższy poziom języka wyrażającego aspekty bezpieczeństwa, które mogą być weryfikowane. Między komponentami mogą występować zależności, które należy uwzględnić w procesie oceny.

Kluczem do prawidłowego przedstawienia procesu oceny przykładowego Zadania Zabezpieczeń opisanego w dalszej części referatu jest omówienie budowy komponentu uzasadniającego zaufanie. Składa się on z elementów trzech typów D, C oraz E:

- elementarna akcja konstruktora (*ang. Developer Action Element*) – określa czynności, za które odpowiada konstruktor; oznaczana jest literą **D** na końcu nazwy elementu; zwykle określa, że powinien on „coś" opracować, „coś" dostarczyć, nie precyzując przy tym, jaką to ma mieć postać – określa to dopiero kolejny typ elementu,
- element zawartości i prezentacji materiału dowodowego (*ang. Content & Presentation of Evidence Element*) – określa wymagania, co do wykazu informacji źródłowych, ich zawartości oraz postaci, dostarczanych przez konstruktora, a potrzebnych dla oceniającego do prowadzenia oceny (np. mogą to być: zawartość wybranego rozdziału dokumentacji użytkowej, opis procedury instalacji, urządzenie, test itp.); oznaczany jest literą **C**,

- elementarna akcja oceniającego (*ang. Evaluator Action Element*) – określa czynności, które wykonuje oceniający – sprawdza, czy konstruktor dostarczył to „coś" i czy ma „to" odpowiednią zawartość i postać; takie elementy oznaczane są literą **E**.

6. Rodzaje ocen i werdykt końcowy

Wspólne Kryteria wraz z Metodologią Oceny umożliwiają realizację trzech rodzajów ewaluacji: ocenę Profilu Zabezpieczeń, ocenę Zadania Zabezpieczeń oraz ocenę Przedmiotu Oceny.

Ocena Profilu Zabezpieczeń stanowi sprawdzenie zgodności opracowanego PP z kryteriami. Celem jest tu ocena, czy dokument jest kompletny, spójny wewnętrznie i poprawny pod względem technicznym, przez co może stanowić bazę do tworzenia rodziny podobnych TOE (produktów, systemów) lub innych PP. Ewaluacja odbywa się zgodnie z kryteriami zawartymi w 3 części CC, głównie w rozdziałach 3 oraz 4.

Ocena Zadania Zabezpieczeń – dokument ST jest opisem produktu lub systemu, w którym identyfikuje się funkcje zabezpieczające, możliwe mechanizmy bezpieczeństwa, które wprowadzają w życie polityki bezpieczeństwa instytucji i przeciwstawiają się zdefiniowanym zagrożeniom w ramach zdefiniowanych założeń. Oczekuje się od ST zdefiniowania miar zapewniających zaufanie do produktu lub systemu, który poprawnie przeciwstawia się zagrożeniom i wprowadza w życie polityki bezpieczeństwa instytucji.

Ocena dokumentu stanowi sprawdzenie zgodności opracowywanego ST z kryteriami. Również i w tym przypadku celem jest sprawdzenie, czy dokument ST jest kompletny, spójny wewnętrznie i poprawny pod względem technicznym oraz ponadto, jeśli opracowano go na podstawie PP, to dodatkowym celem jest wykazanie jego zgodności z tym profilem. Wymagania ST po pozytywnej ocenie stanowią podstawę do rozpoczęcia ewaluacji samego TOE. Ocena ST odbywa się zgodnie z kryteriami zawartymi głównie w rozdziałach 3 oraz 5 trzeciej części Wspólnych Kryteriów.

Ocena TOE – mając ocenione Zadanie Zabezpieczeń ST jako dokument odniesienia, można przystąpić do oceny opracowywanego na jego podstawie produktu lub systemu (TOE). Celem jest wykazanie, że Przedmiot Oceny spełnia wymagania na zabezpieczenia zawarte w jego Zadaniu Zabezpieczeń. Ocena TOE odbywa się zgodnie z zadeklarowanym przez konstruktora poziomem uzasadnionego zaufania EAL.

Na potrzeby przykładu oceny Zadania Zabezpieczeń aplikacji SecOffice przedstawione dalej tabele 1 i 2 dotyczą tylko jednego, wybranego komponentu, który służy do oceny otoczenia zabezpieczeń Przedmiotu Oceny.

W tabeli 1 zawarto opis podejmowanych działań oznaczonych literami C, D i E zgodnie ze sposobem opisu elementów uzasadniających zaufanie.

Tabela 1

Wymagania na otoczenie zabezpieczeń

Rodzina i jej cele	Charakterystyka podejmowanych działań	Komponent uzasadniający zaufanie
Otoczenie zabezpieczeń Dokładne zrozumienie przez wszystkie strony rozwiązywanego problemu bezpieczeństwa	D – dostarczenie opisu otoczenia zabezpieczeń TOE jako część ST, C – opis otoczenia powinien identyfikować i wyjaśniać: założenia dotyczące zamierzonego użytkowania TOE, znane lub zakładane zagrożenia dla aktywów, polityki bezpieczeństwa instytucji, E – potwierdzenie, że dostarczone informacje spełniają wszystkie wymagania dotyczące zawartości i prezentacji materiału dowodowego, że sformułowanie opisujące środowiska zabezpieczeń TOE jest spójne i wewnętrznie zgodne.	**ASE_ENV.1** Zależny od: brak zależności

Werdykt końcowy – najmniejszą „jednostką" podlegającą werdyktowi jest elementarna akcja oceniającego, składająca się ze zbioru jednostek oceny. W tym miejscu można mówić o werdykcie cząstkowym. Stosuje się trzy możliwe wartości dla werdyktów: **FAIL** - negatywny, **PASS** - pozytywny, **INCLSV** – nierozstrzygnięty (*ang. Inconclusive*), co oznacza, że nie można było wykonać wszystkich czynności, jednostek oceny.

Werdykty ulegają specyficznej kumulacji. Werdykt dla komponentu uzasadnionego zaufania uwzględnia werdykty dla wszystkich jego elementarnych akcji oceniającego, werdykt dla klasy uwzględnia werdykty wszystkich jej komponentów, zaś werdykt końcowy obejmuje: werdykt dla klas - *APE* (dla PP) albo *ASE* (dla ST); werdykty dla zestawu komponentów pozostałych klas, wyspecyfikowanych dla zadeklarowanego poziomu EAL.

Wynik ewaluacji jest pozytywny tylko wówczas, gdy wszystkie akcje oceniono pozytywnie. Warunkiem uzyskania certyfikatu musi być pozytywna weryfikacja ocen uzyskanych w toku ewaluacji prowadzonej wg CC. Proces certyfikacji polega na niezależnej kontroli wyników oceny.

Metodyka postępowania weryfikującego oceny ewaluacji oraz procesy certyfikacji znajdują się poza zakresem Wspólnych Kryteriów (CC) i leżą zwykle w kompetencjach specjalnie powołanych do tego celu organów państwowych.

Dla komponentu *ASE_ENV.1* z tabeli 1 przedstawiono dodatkową tabelę 2, w której zawarto elementarne akcje oceniającego, elementy ocenianego materiału dowodowego wraz z odpowiadającymi im jednostkami oceny. Jednostki oceny zostały dodatkowo wzbogacone o opis podstawowej czynności (w postaci pogrubionej kursywy), którą musi wykonać oceniający w celu poprawnego zbadania dowodu i wydania oceny. W wielu jednak przypadkach podstawowa czynność jest niewystarczająca dla wydania poprawnej jednostki

oceny przez oceniającego, dlatego też w części 2 CEM w rozdziale dotyczącym klasy *ASE* dla każdej jednostki oceny dodano szereg wskazówek i interpretacji pomagających w dużym stopniu w wydaniu prawidłowej oceny. Ze względu na dużą liczbę tych wskazówek w tabeli 2 przedstawiono tylko podstawowe czynności oceniającego, wskazujące jedynie kierunek prowadzenia procesu oceny.

Celem zakresu komponentu *ASE_ENV.1* jest określenie, czy wyrażone w ST otoczenie zabezpieczeń TOE zapewnia przejrzystą i zgodną definicję problemu zabezpieczeń.

W tabeli 2 umieszczono elementarne akcje oceniającego składające się na zakres komponentu oraz jednostki oceny dotyczące odpowiednich fragmentów materiału dowodowego.

Tabela 2

Ocena otoczenia zabezpieczeń *(ASE_ENV.1)*

Element treści i formy	Elementarna akcja oceniającego	Jednostka oceny
ASE_ENV.1.1C	ASE_ENV.1.1E	**ASE_ENV.1-1** Oceniający ***powinien zbadać (ang. shall examine)*** sformułowanie otoczenia zabezpieczeń TOE, czy identyfikuje i wyjaśnia wszystkie założenia dotyczące zamierzonego użytkowania TOE i środowiska, w którym będzie eksploatowane. Oceniający określa, czy założenia dotyczące środowiska użycia spełniają aspekty sprzętowe, osobowe oraz łączności z innymi systemami lub produktami IT.
ASE_ENV.1.2C		**ASE_ENV.1-2** Oceniający ***powinien zbadać*** sformułowanie otoczenia zabezpieczeń TOE, czy identyfikuje i wyjaśnia wszystkie zagrożenia. Jeśli cele zabezpieczeń dla TOE i środowiska wywodzą się tylko z założeń i polityk bezpieczeństwa instytucji, to sformułowanie zagrożeń nie musi być obecne w ST. W takim przypadku nie stosuje się jednostki oceny uważając, że jest pozytywna.
ASE_ENV.1.3C		**ASE_ENV.1-3** Oceniający ***powinien zbadać*** sformułowanie otoczenia zabezpieczeń TOE, czy identyfikuje i wyjaśnia wszystkie polityki bezpieczeństwa instytucji. Jeśli cele zabezpieczeń dla TOE i środowiska wywodzą się tylko z założeń i zagrożeń, to polityki bezpieczeństwa instytucji nie muszą być obecne w ST. W takim przypadku nie stosuje się jednostki oceny uważając, że jest pozytywna.
	ASE_ENV.1.2E	**ASE_ENV.1-4** Oceniający ***powinien zbadać***, czy sformułowanie otoczenia zabezpieczeń TOE jest spójne, tzn. czy tekst i struktura sformułowania są zrozumiałe dla docelowych odbiorców dokumentu (np. oceniających i klientów).
		ASE_ENV.1-5 Oceniający ***powinien zbadać***, czy sformułowanie otoczenia zabezpieczeń TOE jest wewnętrznie zgodne. Przewodnik po analizie zgodności zawarty jest w aneksie B.3 CEM [5].

7. Przykład oceny wybranego fragmentu Zadania Zabezpieczeń aplikacji SecOffice

Przykład oceny ST został przedstawiony na podstawie fragmentu Zadania Zabezpieczeń aplikacji SecOffice [11], dotyczącego identyfikacji otoczenia zabezpieczeń TOE.

Program SecOffice przeznaczony jest do szyfrowania i podpisywania dokumentów elektronicznych, dokonuje on zabezpieczenia dokumentów bezpośrednio z poziomu edytora Microsoft Word lub z poziomu menu kontekstowego Eksploratora Windows, wykorzystując systemową bibliotekę funkcji kryptograficznych CryptoAPI.

Zgodnie z tabelą 1 oraz 3 częścią CC komponent *ASE_ENV.1* weryfikuje, czy problem bezpieczeństwa, który ma być rozwiązany, jest jasno rozumiany przez wszystkie grupy przystępujące do oceny.

Z kolei zgodnie z tabelą 2 oraz 3 częścią CC komponent składa się z następujących elementów D, C i E:

Element działalności konstruktora:

ASE_ENV.1.1D - konstruktor powinien dostarczyć sformułowania opisującego otoczenie zabezpieczeń TOE jako część ST. Rozdział 3 - Otoczenie zabezpieczeń TOE [11].

Zawartość i prezentacja elementów materiału dowodowego:

ASE_ENV.1.1C - sformułowanie opisujące otoczenie zabezpieczeń TOE powinno identyfikować i wyjaśniać wszelkie założenia związane z zamierzonym użytkowaniem TOE i środowiskiem używania TOE. Tabela 1 - Identyfikacja założeń [11],

ASE_ENV.1.2C - sformułowanie opisujące otoczenie zabezpieczeń TOE powinno identyfikować i wyjaśniać wszelkie znane lub przypuszczalne zagrożenia dla aktywów, przeciwko którym wymagane będzie zastosowanie zabezpieczeń realizowanych przez TOE lub przez jego środowisko. Tabela 4 = Identyfikacja zagrożeń [11],

ASE_ENV.1.3C - sformułowanie opisujące otoczenie zabezpieczeń TOE powinno identyfikować i wyjaśniać wszelkie polityki bezpieczeństwa instytucji, do których TOE powinien się stosować. Tabela 5 - Identyfikacja polityki bezpieczeństwa [11].

Działalność oceniającego:

ASE_ENV.1.1E - oceniający powinien potwierdzić, że dostarczone informacje spełniają wszystkie wymagania dotyczące zawartości i prezentacji materiału dowodowego,

ASE_ENV.1.2E - oceniający powinien potwierdzić, że sformułowanie opisujące środowisko zabezpieczeń TOE jest spójne i wewnętrznie zgodne.

Mamy zatem dwie akcje oceniającego: *ASE_ENV.1.1E, ASE_ENV.1.2E*, dla których zostaną wydane werdykty cząstkowe. Każdy z tych werdyktów cząstkowych składa się z jednostek oceny *(ang. Work Units)*, które odnoszą się do odpowiednich fragmentów Zadania Zabezpieczeń. Opis jednostek oceny w powiązaniu z odpowiednimi akcjami oceniającego oraz fragmentami ST przedstawiono w tabeli 2. Posługując się zestawieniem z tabeli 2 wykonano ocenę komponentu *ASE_ENV.1*:

1. Werdykt cząstkowy dla ASE_ENV.1.1E

Dotyczy **ASE_ENV.1.1C**

ASE_ENV.1-1 - PASS – ocena pozytywna, ponieważ sformułowanie otoczenia zabezpieczeń TOE identyfikuje i wyjaśnia wszystkie założenia dotyczące zamierzonego użytkowania TOE i środowiska, w którym będzie eksploatowane i przedstawia je w tabeli 1 - Identyfikacja założeń [11]. Założenia spełniają aspekty sprzętowe, osobowe (Tabela 2 - Identyfikacja podmiotów [11]) oraz połączeniowe z innymi systemami.

Dotyczy **ASE_ENV.1.2C**

ASE_ENV.1-2 - PASS – ocena pozytywna, ponieważ sformułowanie otoczenia zabezpieczeń TOE identyfikuje i wyjaśnia wszystkie zagrożenia i przedstawia je w tabeli 4 – Identyfikacja zagrożeń [11].

Dotyczy **ASE_ENV.1.3C**

ASE_ENV.1-3 - PASS – ocena pozytywna, ponieważ sformułowanie otoczenia zabezpieczeń TOE identyfikuje i wyjaśnia wszystkie polityki bezpieczeństwa instytucji i przedstawia je w tabeli 5 – Identyfikacja polityki bezpieczeństwa [11].

ASE_ENV.1.1E - PASS - ocena pozytywna, ponieważ wszystkie jednostki oceny składające się na werdykt cząstkowy były pozytywne.

2. Werdykt cząstkowy dla ASE_ENV.1.2E

Dotyczy **ASE_ENV.1.3C**

ASE_ENV.1-4 - PASS – ocena pozytywna, ponieważ sformułowanie otoczenia zabezpieczeń TOE jest spójne, tzn. tekst i struktura sformułowania są zrozumiałe dla docelowych odbiorców dokumentu (np. oceniających i klientów).

Dotyczy **ASE_ENV.1.3C**

ASE_ENV.1-5 - PASS – ocena pozytywna, ponieważ sformułowanie otoczenia zabezpieczeń TOE jest wewnętrznie zgodne, tzn. sformułowanie zawiera zagrożenia, w których metoda ataku nie wybiega poza możliwości agentów zagrożeń (tabela 4 – Identyfikacja zagrożeń [11]); sformułowanie nie zawiera polityk bezpieczeństwa, które są sprzeczne z występującymi zagrożeniami.

ASE_ENV.1.2E - PASS - ocena pozytywna, ponieważ wszystkie jednostki oceny składające się na werdykt cząstkowy były pozytywne.

3. Werdykt końcowy dla komponentu

ASE_ENV.1 - PASS – ocena pozytywna, ponieważ werdykty cząstkowe: ASE_ENV.1.1E i ASE_ENV.1.2E, składające się na ocenę komponentu spełniły kryteria oceny pozytywnej.

8. Wnioski

Powyższy przykład oceny Zadania Zabezpieczeń dotyczył tylko jednego wybranego komponentu z danej rodziny, który nie był związany zależnościami z innymi komponentami. Jeśli uzmysłowimy sobie, że w celu przeprowadzenia pełnej oceny ST należałoby uwzględnić w naszym przykładzie pozostałych 8 rodzin wraz ze wszystkimi komponentami złożonymi z wielu elementów i ze wszystkimi zależnościami, to będziemy mieli pełny obraz trudności i złożoności procesu oceny zabezpieczeń, a tym samym zrozumiemy celowość prac związanych z budową oprogramowania wspomagającego ten proces.

W dobie coraz większych zagrożeń dla zasobów informatycznych, coraz więcej klientów zwraca uwagę na kwestie bezpieczeństwa produktów teleinformatycznych i wymaga zaprojektowania bądź oceny urządzenia zgodnego z najnowszymi standardami bezpieczeństwa teleinformatycznego. Dlatego też nie należy ustawać w dążeniu do poznania i wdrożenia tych standardów, do szerzenia wiedzy, jak prawidłowo specyfikować funkcjonalność zabezpieczeń w produktach, jakimi miarami należy posługiwać się przy ewaluacji produktu, w jaki sposób mierzyć zaufanie do niego, czy też określać brak w nim zachowań niepożądanych, a także jak projektować bezpieczne produkty.

Ze względu na dużą skalę trudności w implementacji i stosowaniu Wspólnych Kryteriów w procesach projektowania i oceny zabezpieczeń należy położyć duży nacisk na prowadzenie

dalszych prac, mających na celu opracowanie oprogramowania pozwalającego na zautomatyzowanie i usprawnienie tych procesów.

LITERATURA

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, v.2.1, August 1999.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, v.2.1, August 1999.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, v.2.1, August 1999.
4. Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, CEM-97/017, v.0.6, 1997.
5. Common Evaluation Methodology for Information Technology Security, Part 2: Evaluation Methodology, CEM-99/045, v.1.0, August 1999.
6. Białas A.: Wspólne Kryteria – formalna specyfikacja wymagań bezpieczeństwa. IT Security Magazine, 2000, Nr 12.
7. Białas A.: Wspólne Kryteria – metodyka ewaluacji. IT Security Magazine, 2001, Nr 1.
8. Białas A.: Wprowadzenie do problematyki projektowania i oceny zabezpieczeń teleinformatycznych. VIII Konferencja SIECI KOMPUTEROWE – Krynica 2001, Studia Informatica vol. 22, no. 1 (43), Silesian University of Technology Press, Gliwice 2001.
9. Praca zbiorowa pod red. Białasa A.: Metodyka projektowania zabezpieczeń teleinformatycznych. Projekt KBN: 6.T11.073.2001C/5689 pt. System wspomagania projektowania i oceny zabezpieczeń teleinformatycznych, ISS, Chorzów 2002.
10. Praca zbiorowa pod red. Białasa A.: Metodyka prowadzenia badań i oceny środków teleinformatycznych. Projekt KBN: 6.T11.073.2001C/5689 pt. System wspomagania projektowania i oceny zabezpieczeń teleinformatycznych, ISS, Chorzów 2002.
11. Praca zbiorowa pod red. Białasa A.: Opracowanie projektu zabezpieczeń wybranych środków teleinformatycznych zgodnego ze Wspólnymi Kryteriami. Projekt KBN: 6.T11.073.2001C/5689 pt. System wspomagania projektowania i oceny zabezpieczeń teleinformatycznych, ISS, Chorzów 2002.

Recenzent: Dr inż. Andrzej Kwiecień

Wpłynęło do Redakcji 5 kwietnia 2003 r.

Abstract

The paper presents the evaluation methodology, developed under grant from Polish State Committee for Scientific Research (KBN), for conducting evaluations which apply Common Criteria (ISO/IEC 15408).

The paper describes the main principles and assumptions of the IT security evaluation process, which are: appropriateness, impartiality, objectivity, repeatability and reproducibility, soundness of results, cost-effectiveness, methodology evolution, re-usability.

The general model of the methodology was presented with the roles and responsibilities of the parties involved in the evaluation process (Figure 1).

The paper also presents high-level overview of the evaluation process which can be divided into three stages which may overlap: preparation - in this stage initial contact is made between the sponsor and the evaluator; conduct - in this stage the evaluation is performed; conclusion - in this stage the evaluation results are delivered.

All evaluations, whether of a PP or TOE (including ST), have two evaluator tasks in common: the input task and the output task. These two tasks, which are related to management of evaluation evidence and to report generation, are described in the paper.

The formal notation of security properties were described including security functional components, EALs – Evaluation Assurance Levels, security assurance components with description of its elements: Developer Action Element, Content & Presentation of Evidence Element and Evaluator Action Element (Table 1).

The paper also presents types of evaluations, the way of getting certificates and specifies the work units (Table 2) applied in the evaluation process example.

The Security Target of SecOffice application (used to encryption and digital signature of documents and files) with the component concerning security environment were shown as an example of the process evaluation in this paper.

Adres

Dariusz ROGOWSKI: Instytut Systemów Sterowania, ul. Długa 1-3, 41-506 Chorzów, Polska, drogowsk@iss.pl .