1.2 Zarządzanie materiałem dowodowym w cyklu życia systemu

Jednym ze sposobów zarządzania materiałem dowodowym jest model oparty na wskazywaniu dowodów w ramach ukierunkowanych norm bezpieczeństwa oprogramowania. Przyjęcie takiego podejścia do zagadnienia zarządzania materiałem dowodowym wymaga dużej liczby dowodów bezpieczeństwa systemu generowanych w oparciu o wymogi projektowanego oprogramowania. Istotna jest też skuteczna ocena dowodów w celu optymalizacji ich ilości. Ukierunkowane normy bezpieczeństwa oprogramowania nie kwestionują roli argumentów ponieważ to one nadają sens dowodom ale to właśnie dowody dają pewność bezpieczeństwa systemu. Ostatecznie wymagane jest aby wykazać że produkt jest akceptowalnie bezpieczny co jest możliwe tylko poprzez wskazanie bezsprzecznych na to dowodów.

Istotną kwestią w kontekście generowania dowodów jest wielkość projektu. Jeśli zakres prac jest niewielki dużo łatwiej zidentyfikować liczbę dowodów wystarczających do potwierdzenia zakładanej cechy systemu. Ryzyko niskiej efektywności a nawet bezużyteczności działań podejmowanych w zakresie identyfikacji i weryfikacji dowodów zwiększa się wraz z wydłużeniem w czasie procesów potrzebnych do wytworzenia oprogramowania. Efektem wzrostu takiego rodzaju ryzyka w projekcie jest zwiększenie kosztów i przekroczenie terminu jego wykonania o czas który jest niezbędny do zagwarantowania właściwej oceny materiału dowodowego. Jeśli zbyt dużo czasu zajmie nam ocena zebranych dowodów niemal na pewno konieczne będzie okrojenie czasu potrzebnego przy innych czynnościach zmierzających do ograniczenia ryzyka. Konieczność efektywnego zarządzania materiałem dowodowym wymusza także kwestia uzyskania w określonym czasie akceptacji organów nadzorujących proces wytwórczy.

Istotnym elementem w analizy jest argument o bezpieczeństwie. Wymagane jest jego systematyczne kontrolowanie pod względem ważności w sposób manualny. Pomimo wprowadzenia standardów strukturyzujących m.in. GSN, CAE co pozowała na bardziej rygorystyczne analizowanie argumentu nieodzowna jest recenzja tego elementu wykonana przez ludzi. Przyjmuje się że argument musi być przedstawiony w sposób czytelny i zrozumiały. Obarczanie argumentu niepotrzebnymi szczegółami może skutkować że będzie on rozpatrywany w sposób fragmentaryczny z dużą dozą ryzyka pomijania istotnych interakcji zachodzących w jego wnętrzu. Skomplikowane określenie tego co jest argumentem może przyczynić się do podwyższenia trudności we właściwym zrozumieniu i w rezultacie błędnej interpretacji, ewentualnie zupełnego odrzucenia w trakcie weryfikacji. Rozwiązaniem w unikaniu podobnych sytuacji może być przyjęcie zasad abstrakcji oraz oddzielenia wymagań od realizacji tzn. argument musi zdefiniować wymagania dla różnych rodzajów dowodów ale jednocześnie pozostając niezależnym od szczegółów realizacji dowodów. Takie podejście umożliwia uzgodnienie argumentu bezpieczeństwa we wczesnym cyklu życia systemu. Zakończenie procedury udowadniania wiarygodności wymaga przedstawienia sprawozdania dotyczącego dowodów śledzących procesy powiązane z tym argumentem.

Częstym problemem obserwowanym zwłaszcza w realizacji dużych projektów jest konieczność uzyskania akceptacji argumentu bezpieczeństwa ze strony wielu zainteresowanych stron m.in. organu nadzoru operacyjnego, integratora systemów, producenta oprogramowania i niezależnego eksperta w dziedzinie bezpieczeństwa. Istnieje zatem konieczność uzgodnienia argumentu na wczesnym etapie cyklu życia systemu w ramach planowania harmonogramu zarządzania bezpieczeństwem i tworzenia dokumentacji technicznej w tym planu rozwoju oprogramowania etapy jego weryfikacji. Przeprowadzanie uzgodnień w zakresie argumentu jest możliwe na późniejszym etapie rozwoju projektu jednakże należy wówczas mieć na uwadze wzrost trudności w realizacji potrzeb w zakresie zapewnienia bezpieczeństwa.