# Ocena ryzyka oprogramowania dla przyrządów pomiarowych w metrologii prawnej

***Streszczenie* – W Europie, przyrządy pomiarowe podlegające prawnej kontroli są odpowiedzialne za roczne obroty w wysokości 500 bilionów Euro i zanim będą mogły być użyte muszą przejść ocenę zgodności z uwzględnieniem dyrektyw unijnych lub przepisów krajowych. Przyrządy pomiarowe są dziś często zintegrowane z sieciami otwartymi i nawet działają w obszarach „chmury obliczeniowej” i Internetu. Ponieważ oprogramowanie jest jednym z kluczowych składników takich urządzeń, w niemieckim instytucie metrologicznym Physikalisch-Technische Bundesantalt opracowywana jest metoda uzyskania ryzyka i obliczeń aktualnych zagrożeń związanych z oprogramowaniem. Metoda wykorzystuje strukturę i łączy w sobie elementy norm międzynarodowych ISO / IEC 27005 i 15408. Może ona być przydatna dla organów oceny zgodności i przemysłu oraz wspierać jednocześnie porównywalność wyników oceny ryzyka. Pomimo, że koncentruje się ona na metrologii prawnej, metoda ma zastosowanie w innych obszarach, w których również wymagana jest ocena ryzyka oprogramowania.**

I. WPROWADZENIE

PEWNE typy przyrządów pomiarowych, jak gazomierze, taksometry, pompy paliwowe, mierniki wilgotności ziarna podlegają prawnej kontroli w Unii Europejskiej. Przed pojawieniem się ich na rynku, takie przyrządy pomiarowe muszą przejść ocenę zgodności zgodnie z dyrektywą przyrządów pomiarowych (MID) 2014/32 / UE [1]. Cały obszar przyrządów pomiarowych włączając w to szczególne pomiary regulowany jest przez ich prawodawstwo narodowe lub Europejskie zwane metrologią prawną. Zgodnie z szacunkiem, około czterech do sześciu procent całości wpływów w krajach Europejskich jest powiązanych z metrologią prawną. W samych Niemczech zainstalowanych jest 130 milionów takich przyrządów. Są one odpowiedzialne za transakcje warte około 157 bilionów Euro każdego roku. Dla uzyskania szczegółów związanych rolą metrologii prawnej, patrz [2].

W większości przypadków, oceny zgodności wykonywane się poprzez tzw. jednostki notyfikujące, które udowodniły, że mają do dyspozycji "(a) pracowników posiadających wiedzę techniczną oraz wystarczające i odpowiednie doświadczenie do realizacji zadań związanych z oceną zgodności, (b) opisy procedur, zgodnie z którymi została przeprowadzona ocena zgodności w celu zagwarantowania przejrzystości i powtarzalności tych procedur "[1]. Jednym z takich jednostek notyfikujących, które przeprowadzają ocenę zgodności jest Physikalisch-Technische Bundesanstalt (PTB), niemiecki krajowy instytut metrologii. Sama ocena jest prowadzona zgodnie z kombinacją modułów (od A do H1), które obejmują różne role producentów i jednostek notyfikujących [1]. Dla większości z tych modułów, wprowadzony został ogólny nowy wymóg w 2014 roku w sprawie dokumentacji przedkładanej przez producenta. Stwierdza on: "Dokumentacja musi umożliwiać dokonanie oceny zgodności przyrządu z odpowiednimi wymaganiami oraz obejmuje odpowiednią analizę i ocenę ryzyka (ryzyk)." Taka ocena ryzyka dotyczy nie tylko spełnienia przez przyrząd wymagań pomiaru fizycznego ale również oprogramowania metrologicznego działającego na nim. W tym kontekście, harmonizacja między europejskimi jednostkami notyfikującymi staje się oczywiście niezbędna w celu zapewnienia sprawiedliwej i porównywalnej oceny ryzyka oprogramowania w ramach wspólnej strefy handlowej. W opracowaniu tym, projekt oceny ryzyka oprogramowania zakłada

* korzystanie w miarę możliwości z ustalonych międzynarodowych standardów,
* identyfikuje ryzyko z powtarzalnymi wartościami numerycznymi dla lepszej porównywalności wyników oceny.

Pozostała część opracowania skonstruowana jest w następujący sposób: W części II dołączono przegląd metod odnoszących się do obszaru oceny ryzyka oprogramowania. W celu uzyskania powtarzalności wyników analizy, wymagane jest jasne określenie aktywów i zagrożeń dla tych aktywów. W rozdziale III zawarte jest wyprowadzenie takich aktywów z wymagań MID. Algorytmiczny opis proponowanej tutaj metody oceny ryzyka, można znaleźć w rozdziale IV. Później nowe podejście porównywane jest z innymi istniejącymi metodami opartymi na dwóch realnych przykładach w rozdziale V. Rozdział VI podsumowuje opracowanie i zawiera przegląd planowanej przyszłej pracy.

II PRZEGLĄD ISTNIEJACYCH METOD

Zanim przedstawiona zostanie lista odniesiona do oceny ryzyka oprogramowania, konieczne jest jasne określenie, jaki rodzaj oceny ryzyka jest wymagany w ramach MID. Dyrektywa ustanawia wspólną podstawę, wymieniając szereg zasadniczych wymagań, które wszystkie przyrządy pomiarowe muszą spełniać. Ponieważ najważniejszym celem MID jest zapewnienie swobodnego i uczciwego handlu, a także realizacja celu ochrony konsumenta, zasadniczo wymagania są ukierunkowane przede wszystkim na ochronę wyników pomiarów przed przypadkową i celową manipulacją i aby zarówno prawidłowe wyniki pomiarów i wykryte manipulacje były identyfikowalne. Szczegóły można znaleźć w Rozdziale III. W tym kontekście, termin ryzyko może być postrzegany jako iloczyn prawdopodobieństwa, że zasadnicze wymagania nie są już spełnione i wynikają skutki prawne z takiego naruszenia MID. Warto zauważyć, że straty finansowe nie powinny być skojarzone z ryzykiem, podstawą analizy są wymagania.

1. *ISO/IEC 27005*

Prawdopodobnie najważniejszym jest wspomnieć rodzinę standardów ISO / IEC 27000, które odnoszą się do wszystkich aspektów systemu zarządzania bezpieczeństwem (ISMS). Zgodnie z normą ISO / IEC 27005 [3], "ryzyko jest połączone z konsekwencjami, które wynikają z wystąpienia niepożądanego zdarzenia i prawdopodobieństwa wystąpienia zdarzenia." Tak więc, konieczne są trzy elementy do obliczania ryzyka, a mianowicie

* Lista niepożądanych zdarzeń,
* Konsekwencje wynikające z takich zdarzeń,
* Prawdopodobieństwa wystąpienia poszczególnych zdarzeń.

W celu uzyskania wszystkich trzech komponentów [3] zawiera szczegółowe informacje na temat ogólnych procedur do wyprowadzenia oceny ryzyka. Standardowe miejsce oceny ryzyka w łańcuchu logicznym obejmującym ustanowiony kontekst oceny ryzyka i postrzegania ryzyka, gdzie ocena ryzyka składa się z identyfikacji ryzyka, estymacji obliczeń ryzyka.

W fazie identyfikacji ryzyka, aktywa mają być identyfikowane jako pierwsze. Pochodzą one z „listy ustanowienia właścicieli, lokalizacji, funkcji”, z listy wynikają zarządzane aktywa. Następnie, dla każdego możliwego aktywa na podstawie przeglądu incydentów zbierane są informacje o zagrożeniach, kątach właścicieli aktywów, i możliwych kategoriach zagrożeń zewnętrznych. Zagrożenia te odpowiadają "niechcianych wydarzeniom", o których mowa powyżej. Kolejny krok polega na identyfikacji istniejących mechanizmów kontroli ryzyka, które mogą, na przykład, być ustalone z dostarczonej dokumentacji. Identyfikacja ryzyka zakończona jest przez identyfikacji luk w zabezpieczeniach, które mogą być wykorzystane do realizacji pewnych zagrożeń. W tym kontekście, luka może zaszkodzić tylko wtedy, gdy jest wykorzystana do realizacji zagrożenie. Tym samym, zagrożenia bez wskazania wrażliwego celu nie stanowią zagrożenia.

Kolejna część ISO / IEC 27005, dotyczy oszacowania ryzyka, jest to prawdopodobnie najbardziej istotne w kontekście tego artykułu. Standard odnosi się zarówno do jakościowych i ilościowych obliczeń prawdopodobieństwa ryzyka, gdzie podejście ilościowe „używa skali wartości liczbowych zarówno dla skutków i prawdopodobieństwa, z wykorzystaniem danych pochodzących z różnych źródeł.” Takie wartości liczbowe niezbędne są dla zapewnienia porównywalności między wynikami oceny ryzyka dla różnych produktów prowadzonych przez różnych egzaminatorów. Aby wyprowadzić rzeczywiste prawdopodobieństwa, ISO / IEC 27005 po pierwsze przypisuje pewne skutki lub konsekwencje incydentom, które mogłyby mieć efekt w realizacji zagrożeń w rozumieniu wykorzystania luk. Możliwe przykłady oddziaływania obejmują utratę poufności pewnych aktywów, jak również naruszenie integralności aktywów. W końcowym etapie, szacowane jest prawdopodobieństwo, z którym realizowane jest zagrożenie. Ważne czynniki, w tym kontekście, to częstotliwość, przy której występują pewne zagrożenia w życiu i trudności wykorzystania luki. Dla celowego wykorzystywania zagrożeń, ISO / IEC 27005 sugeruje wycenę motywacji i możliwości, zasobów dostępnych agresorowi, jak również postrzeganie poszczególnych luk. Podejście to będzie później przekształcona w sekcji IV, w którym pewne aspekty ISO / IEC 27005 znajdują odzwierciedlenie w podejściu oceny ryzyka tutaj przedstawionej. Niemniej, standard nie określa modelu odniesienia do numerycznego obliczenia poszczególnych prawdopodobieństw zagrożenia. Standard pozostawia użytkownikowi wybór takiego modelu. Jedną z możliwych metod obliczania ryzyka ilościowego, na przykład, można znaleźć w [4], w którym autor proponuje zdefiniowanie ryzyka jak funkcji prawdopodobieństwa opisujących prawdopodobne zyski lub straty wynikające z incydentów bezpieczeństwa. Końcowymi elementami oceny ryzyka zgodnie z normą ISO / IEC 27005 jest ocena poziomu ryzyka i obliczenia ryzyka. Celem tych działań jest ustalanie zidentyfikowanych ryzyk zgodnie z wcześniej ustalonymi kryteriami oceny.

1. *Przewodnik WELMEC 5.3*

W celu zharmonizowania pracy jednostek notyfikujących w Europie powstało szereg nieoficjalnych przewodników w ramach przedsiębiorstw europejskiej metrologii prawnej (WLMEC). Przewodnik 5.3 „Przewodnik oceny ryzyka dla nadzoru rynku” zajmuje się oceną ryzyka z punktu widzenia nadzoru rynku i pochodzi z rozporządzenia 765/2008 / WE [5]. Głównym celem „jest zrozumienie wpływu przyrządu na użytkownika końcowego / konsumenta”. Przewodnik ustala listę kryteriów oceny, która powinny pomóc „organowi nadzoru rynku w określeniu priorytetów i decyzji o wyborze strategii, aby osiągnąć swoje cele”. Ponieważ podręcznik jest skierowany wyłącznie do organów nadzoru rynku, oczekiwany wpływ nie jest jasno określony, lecz obejmuje wszystko, od "skutków ekonomicznych, zdrowia publicznego, zaufania konsumentów [do] zagadnień prawnych" [6]. Nawet jeśli rozważane są kwestie prawne, spektrum przewodnika jest ciągle zbyt szerokie, aby obiektywnie oceniać oprogramowanie przyrządów pomiarowych. Zamiast tego, przewodnik zawiera wyraźny przepis, do ostatecznego obliczenia ryzyka związanego z brakiem zgodności, ale nie zapewnia środków do obliczania poszczególnych prawdopodobieństw zagrożeń.

1. *Van Deursen et al. „Ocena ryzyka oparta na kodzie źródłowym oprogramowania”*

Jednym z rozwiązań, które pozbawione są tej wady jest van Deursen et al. w [7]. Ocena ryzyka jest zdefiniowana jako „niezależna ocena ryzyka związana z budową, eksploatacją i utrzymaniem oprogramowania”. Metoda, która oblicza ryzyko w oparciu o tak zwane fakty podstawowe i wtórne, gdzie fakty podstawowe są uzyskane automatycznie z analizy kodu źródłowego, a fakty wtórne uzyskane z zastosowania kwestionariuszy użytkownika. Przede wszystkim do identyfikacji podsystemów potrzebne są fakty podstawowe, które pokazują możliwości zwykle nie występujące w systemach oprogramowania. Po faktach podstawowych wykorzystane są fakty wtórne i wówczas może być obliczony ostateczny wynik. Sposób ten łatwo może być wykorzystany w metrologii prawnej. Jednak kod źródłowy nie jest zazwyczaj wymaganą częścią dokumentacji oceny zgodności MID.

1. *Model oceny ryzyka oprogramowania” Foo et al.*

Inny sposób, aby obiektywnie ocenić i porównać ryzyko związane z oprogramowaniem został przedstawiony przez Foo et al. W [8]. Podstawowa abstrakcyjna technika wykorzystywana przez autorów to model oceny ryzyka oprogramowania (SRAM), który zbudowany jest w oparciu o obszerny kwestionariusz, na który odpowiada asesor ryzyka oprogramowania. W [8] termin ryzyko zdefiniowany jest jako "czynniki, które mogą spowodować koszt opóźnienia dostawy lub niska jakość oprogramowania." Nie mniej jednak autorzy wymieniają poziom pracowników produkcji, elastyczność harmonogramu dostaw i najistotniejsze złożoność oprogramowania, mające znaczący wpływ na obliczenia ryzyka. W kontekście oceny zgodności MID, pierwsze dwa źródła informacji są bez znaczenia, ponieważ MID nie dotyczy procesów biznesowych. Złożoność oprogramowania nie może być wykorzystana z uwagi na brak dostępu informacji. Ponadto, osoba oceniająca ryzyko w podejściu SRAM musi mieć dostępu do zasobów, takich jak statystyki kodu źródłowego i błędów, które nie są dostępne dla oceniającego MID. Dla porównania, opis podejścia oceny ryzyka w odniesieniu do przyrządów pomiarowych z podobnym zakresem obejmujący cały cykl życia urządzenia, można znaleźć w [9].

1. *Sadiq et al. „Ocena ryzyka oprogramowania i proces obliczeniowy (SREAP) wykorzystujący podejście modelu podstawowego”*

W [10] zaproponowana był inna metoda oceny ryzyka oprogramowania również sterowana modelem. Sadiqa et al. opisują w niej ocenę ryzyka oprogramowania i ocenę procesu (SRAEP), który oparty jest na ocenie ryzyka oprogramowania i modelu oceny (SRAEM). Ich podejście ukierunkowane jest na podkreślenie zagrożeń dla powodzenia projektu oprogramowania, a nie zagrożeń dla produktu gotowego oprogramowania. Nie mniej jednak, wiele przydatnych kroków formalizacji włączonych jest w ich metody, które mogą być wykorzystane w przyszłości. Z tych powodów, podstawowe kroki będą przywołane tutaj.

Według autorów jest dwojaka motywacja korzystania z modelu opartego o strategię oceny:

* Za pomocą modelu można sformułować precyzyjne opisy systemu docelowego, jego kontekst i zabezpieczenia. Są to warunki wstępne dla przeprowadzenia oceny ryzyka.
* Technologia modelowania umożliwia bardziej precyzyjną dokumentację wyników oceny ryzyka i założeń, od których zależy ich poprawność. Oczekuje się obniżenia kosztów utrzymania poprzez zwiększenie możliwości ponownego wykorzystania dokumentacji.

Sam SRAEP może być podzielony na dwa etapy: identyfikacji związku z analizą i identyfikacji samych ryzyk. Sadiqa et al. dzielą tutaj identyfikację kontekstową na identyfikację obszarów zainteresowania, opis i ocenę aktywów i, w końcu, na wskazanie wymagań bezpieczeństwa. Te trzy kroki będą ponownie zastosowane podczas pozyskiwania aktywów, patrz rozdział III i w metodę oceny ryzyka, która jak opisano w rozdziale IV jest tam zaproponowana. Przed rozpoczęciem z analizy ryzyka, SRAEP wymaga od oceniającego zdobycie szczegółowej wiedzy na temat celu analizy. Na podstawie tej wiedzy, wszystkie kwestie bezpieczeństwa związane z oprogramowaniem powinny być omówione nawiązując do luk lub wyników kontroli podatności opierając się na narzędziach.

*F. ISO/IEC 15408 (Common Criteria) (wspólne kryteria)*

Międzynarodowy standard bezpieczeństwa oprogramowania, który wyraźnie nie odwołuje się do oceny ryzyka to ISO / IEC 15408 znany również jako "Common Criteria" (CC) [11].

W CC, zdefiniowany jest zestaw wymagań funkcjonalnych bezpieczeństwa, co może być wykorzystane do opisu zarówno wymagań określonych w formie Profilu Ochrony i specyfikacji produktu w postaci Celów bezpieczeństwa. Implementacja celu ochrony tj. testowanie produktu odniesione jest do celu ochrony (Target of Evaluation (TOE)). Standard zawiera także listę składników bezpieczeństwa, wybrany podzbiór, który także jest włączony do tak zwanego profilu ochrony i celów ochrony. Te składniki bezpieczeństwa są następnie użyte do zatwierdzenia projektu, rozwoju i ostatecznie do kompletacji samego produktu IT. W ten sposób sprawdzane są składniki bezpieczeństwa nie opisane w CC lecz w Common Evaluation Methodology (CEM)[12], która towarzyszy CC. Dwa bloki CC z danymi zawartymi w CEM są tutaj szczególnie interesujące: po pierwsze każdy cel ochrony zawiera definicję problemu ochrony, w której zdefiniowane są zagrożenia ochrony. CC na początku prezentuje listę aktywów w postaci obiektu lub informacji danej przez wartości takie jak autentyczność, integralność dostępność, które powinny być chronione. Pewne aspekty produktu IT mogą także wywoływać aktywa, gdy odgrywają integralną rolę w realizacji funkcjonalności ochrony. Są one odniesione do aktywów wtórnych. Oba typy aktywów są sprawdzane i wymieniane w definicji problemu ochrony. Następnie badane są i opisywane w sposób semi-formalny możliwe scenariusze zagrożeń i niekorzystne działania. Połączenie czynnika zagrożenia, aktywów i niekorzystnego wpływu określa się jako zagrożenie. Konstrukcja ta będzie tutaj stosowana dalej, ponieważ ułatwia realizację implementacji wyników oceny ryzyka. Po drugie jedna część sprawdzeń celów ochrony składa się z tak zwanych analiz wrażliwości, które są określone w klasach CC’s AVA\_VAN. Składowe bezpieczeństwa skojarzone z tą klasą umożliwiają sprawdzającemu wykonanie zarówno testów białej i czarnej skrzynki opartych na wiedzy pozyskanej podczas procedur oceny. Analiza wrażliwości stosuje ocenę punktową, gdzie każdej niekorzystnej akcji wykonanej na aktywie obliczana jest, z uwzględnieniem pięciu różnych aspektów, ranga czasu wymaganego dla implementacji ataku na przyrząd, szczegóły w Rozdziale IV. W każdej wymienionej kategorii określona jest punktacja. Na podstawie łącznej sumy wszystkich punktów w TOE oznaczona jest odporność na atak. Odbywa się to przy pomocy macierzy, szczegóły są również w rozdziale IV. Więcej informacji na temat ogólnych mechanizmów analizy wrażliwości również tam się znajduje. Europejski Instytut Norm Telekomunikacyjnych (ETSI) w międzynarodowej organizacji non-profit, publikuje standardy przemysłowe w dziedzinie systemów telekomunikacji. Są one skierowane do producentów komunikacji urządzenia i sieci operatorów. Jednym z tych standardów jest ETSI TS 102 165-1 "Telekomunikacja i Internet usług konwergentnych i protokoły dla zaawansowanych informacji o sieci " [13] (TISPAN), przy czym w części 1 "Sposób i proforma na zagrożenia, ryzyka, analizę wrażliwości "są uszczegółowione.   
Tzw. specyfikacja techniczna opisuje podejście do oceny ryzyka składające się z dziewięciu poszczególnych etapów, które obejmują wszystko, co definiuje urządzenia do badania (TOE) w ustaleniu zagrożeń i identyfikacji środków zaradczych. Metoda rozpoczyna się od jasnego zdefiniowania granic TOE oraz określenia bezpieczeństwa funkcjonalnego z wykorzystaniem terminologii wspólnych kryteriów. Po czym identyfikowane są wszystkie aktywa. W [13] mają one pochodzić z jednej z następujących kryteriów: aktywa trwałe, wartości ludzkie lub przechowywane informacje. W rozdziale IV pokazane zostanie, że definicja ta jest bliska wielu aplikacjom poza obszarem systemów telekomunikacji. Co więcej, standard nie opisuje sposobu pozyskania abstrakcyjnych aktywów, przykładowo z instrumentów prawnych. Następne identyfikowane są, możliwe interfejsy ataku w taki sposób, że agent zagrożenia może wprowadzić zagrożenie. W celu oceny prawdopodobieństwa wystąpienia zindywidualizowanego zagrożenia stosuje się opisane wcześniej elementy klas CC AVA\_VAN. Szczegóły na temat metody znaleźć może można w sekcji IV. Według [13] „Zagrożenia dla systemów telekomunikacji są ograniczone i wynikają z niewielkiego zbioru rozpoznanych operacji.” w konsekwencji, [13] wymienia tylko bardzo małą liczbę możliwych zagrożeń, a mianowicie przechwytywanie, manipulacja, odrzucenie, odmowa usługi. Natomiast nadają się do obszaru sieci telekomunikacyjnych, które są ograniczone do urządzeń IT ogólnego przeznaczenia. To samo odnosi się do definicji czynników zagrożeń, gdzie [13] pozwala tylko na bardzo mała liczbę różnych ról. Wreszcie wpływ w kontekście TISPAN określony jest jako funkcja natężenia ataku. Dla przyrządów pomiarowych, omawianych tu, potrzebna jest inna definicja, która będzie przedstawione w rozdziale III. Niemniej jednak, sposób ten ma pewne cechy, które są korzystanie dla scenariusza omawianego tutaj:

* obliczanie prawdopodobieństwa ataku opiera się na klasie CC AVA\_VAN,
* oceny skutków i prawdopodobieństwa ataku występują w oparciu o proste wyniki numeryczne (od 1 do 3 punktów),
* Rozszerzenie klasy AVA\_VAN do wielokrotnych ataków jest wykonywane jednocześnie.

III FORMALNE WYPROWADZENIE WYMAGAŃ BEZPIECZEŃSTWA Z DYREKTYWY 2014/32/EU

Przed rozpoczęciem opisu algorytmu nowej metody oceny ryzyka dla oprogramowania wyprowadzony będzie szczególny zbiór aktywów skojarzony z właściwościami przyrządów pomiarowych. Będą one ponownie użyte w obliczeniach eksperymentalnych. Wyprowadzenie powinno być postrzegane przykładowo jak formalizowanie praw lub wymagań konstrukcyjnych z uwzględnieniem software’u. W scenariuszach nie powiązanych z oceną przyrządów pomiarowych będziemy stosować inne aktywa niż zdrowie ludzkie, wartość monetarna itp. Najnowsza wersja MID wymienia kilka wymagań dotyczących oprogramowania, w postaci zwykłego tekstu, który będzie tutaj sformalizowany.

1. *Przykładowe wyprowadzenie aktywów*

Aktualna procedura definiowania wymagań bezpieczeństwa w oparciu o prawną specyfikację naświetlona zostanie w przykładzie: Załącznik I do MID wymienia tak zwane zasadnicze wymagania wobec przyrządów, które muszą być spełnione przed wprowadzeniem ich na rynek europejski. Jako przykład użyjemy klauzuli 8.4. Mówi ona: „Dane pomiarowe, oprogramowanie, które jest kluczowe dla charakterystyk pomiarowych i ważnych parametrów metrologicznie rejestrowanych lub transmitowanych powinno, być zabezpieczone przed przypadkowym lub celowym zafałszowaniem.” [1, L 96/173]

Wymóg wyraźnie wymienia trzech kandydatów na aktywa, a mianowicie dane pomiarowe, oprogramowanie istotne dla pomiaru i ważne metrologiczne parametry rejestrowane lub transmitowane. Wszystkie trzy aktywa muszą być zabezpieczone przed przypadkowym lub celowym zafałszowaniem. Po pierwsze, może to być interpretowane jako wymóg zagwarantowania integralności tych aktywów. Po drugie jednak intencjonalna zamiana zbioru parametrów także reprezentuje realną drogę do podważenia parametru integralności. Tak więc autentyczność aktywów odnosi się także do wymagania. Nie jest to nic szczególnego w MID ale coś co jest powszechnie zrozumiałe wśród jednostek notyfikujących [14]. W konsekwencji, zbiór danych wartości mierzonych, oprogramowanie istotne dla charakterystyk pomiarowych, oraz parametry metrologiczne są związane z właściwościami bezpieczeństwa integralności i autentyczności. Dostępność oprogramowania jakkolwiek nie jest obowiązkowa, ponieważ przyrząd bez uruchomienia oprogramowania nie może dawać błędnych wyników. Kolejny wymóg związany z oprogramowaniem można znaleźć w Załącznik I do MID, klauzula 7.6. Stwierdza „Kiedy przyrząd pomiarowy wyposażony jest w oprogramowanie, które dostarcza innej jeszcze funkcji niż pomiarowa, oprogramowanie, które jest krytyczne dla charakterystyk metrologicznych, powinno być identyfikowalne i powinno być odporne na niedozwolony wpływ oprogramowania skojarzonego.” [1, L 96/173] Znowu dwa aktywa są szczególnie wymienione. Pierwszy z nich to identyfikacja oprogramowania. Drugim jest niedopuszczenie do wpływu innego programowania, który nie jest obiektem fizycznym lub obiektem IT lecz jest własnością oprogramowania. W języku CC, zakaz wpływu oprogramowania zewnętrznego na oprogramowanie może być wyrażony stwierdzeniem, że niedopuszczalny wpływ będzie niedostępny. To z kolei umożliwia zastosowanie następującego schematu opisu funkcji bezpieczeństwa przez identyfikację dedykowanych własności bezpieczeństwa związanych ze składnikami aktywów.

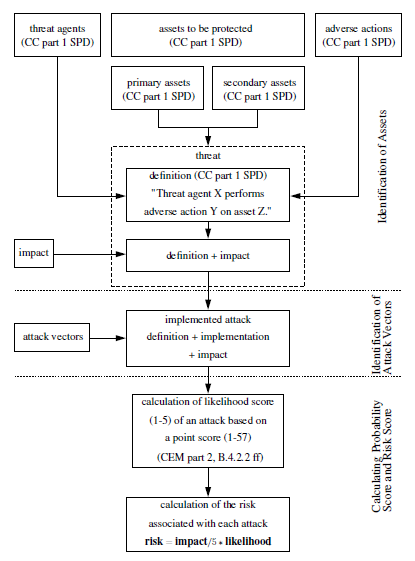
1. *Kompletacja listy aktywów*

Przegląd wszystkich wymagań MID dla oprogramowania w przyrządach pomiarowych można znaleźć w Tabeli I. Są tam wspomniane dwa przykłady tutaj dyskutowane.

Oprócz samego oprogramowania przyrządu, aktywa chronione obejmują identyfikator software’u, pomiar, wyniki lub parametry, które determinują zachowanie przyrządu. Ponadto prezentacja wyników pomiaru jak również prezentacja identyfikatora software’u muszą spełniać specjalne wymagania. Szczegóły, w jaki sposób wymagania te są wypełniane, znaleźć można w [14], gdzie paragrafy z MID tłumaczone są na specjalne wymagania implementacyjne i w tak zwane akceptowalne (techniczne) rozwiązanie. Mimo, że [14] jest zazwyczaj wielkim wyzwaniem zarówno dla programistów jak i ekspertów oprogramowania, tutaj nie będzie stosowane ponieważ nowa procedura oceny ryzyka (patrz rozdział IV) obejmuje ograniczoną, do generycznej i niezależnej postaci, liczbę ustalonych realizacji technicznych.

IV ALGORYTMICZNY OPIS PROCEDURY OCENY RYZYKA

Metoda oceny ryzyka opisana w niniejszym opracowaniu wynika ze struktury zdefiniowanej w [3] i składa się z trzech głównych części, czyli identyfikacji aktywów, identyfikacji wektorów ataków, oraz obliczeń prawdopodobieństwa wystąpienia indywidualnego ataku. Każdy z nich po kolei zostanie teraz opisany. Schemat przepływów, który dla każdego kroku wiąże wszystkie trzy części i komponenty współpracujące, znaleźć można na Rysunku 1.



Rys.1 Przepływ danych proponowanej procedury oceny ryzyka. Uwagi po prawej stronie wskazują podział na trzy główne kroki metody.

*A. Identyfikacja aktywów*

Jak zostało uszczegółowione w Rozdziale III, chronione aktywa mogą być bezpośrednio wyprowadzone z regulacji prawnej dla przyrządów pomiarowych określonych w MID. Jest to zgodne z [3], które stanowi, że proces obliczeń ryzyka może dotyczyć „wymagań prawnych i regulacyjnych oraz zobowiązań umownych” w tym, powinien być uwzględniany „krytyczny wpływ aktywów informacyjnych”. Dodatkowo w definicji aktywa wymagany jest jeden lub więcej modeli agresora, patrz górny prawy róg Rysunku 1. W najprostszym przypadku, jednostka notyfikująca zakłada, że wszyscy uczestnicy rynku są nierzetelni i mają podobną motywację do manipulowania wynikami i przyrządami pomiarowymi. Dotyczy to również producentów lub dystrybutorów takich urządzeń, użytkowników lub opiekunów i klientów. Różnią się oni tylko możliwościami wdrożenia ataku. W związku z tym, procedura oceny ryzyka może wykorzystywać gracza rynkowego o najbardziej zaawansowanej wiedzy i najwyższych umiejętnościach (zwykłego producenta lub użytkownik) jako reprezentanta modelu. Podstawowa struktura zarówno modelu ataku i formuły negatywnego oddziaływania może być znalezione w definicji problemu ochrony opisanej w [11]. Podczas badania określonego przyrządu pomiarowego, może mieć sens indywidualne odróżnienie agresora / uwierzytelnionych użytkowników o różnym poziomie dostępu. Jeśli dla wspomnianego podmiotu rynkowego dostępna jest dana autentykacyjna, wówczas najwyższe prawa dostępu do niej, będą alokowane w modelu agresora. Jedynym podmiotem uważanym za wiarygodny w tym kontekście jest nadzór rynku, który może posiadać poziom administratora przechowującego dane autentykacyjne dla wybranych urządzeń. Innym jeszcze działaniem wykonywanym podczas fazy identyfikacji aktywów jest gromadzenie pewnych niekorzystnych działań, które mogą być przyczyną szkód aktywów. Tutaj również może być zastosowane ogólne podejście CC [11]. Każdy modelowany agresor może uszkodzić jakieś zidentyfikowane aktywa poprzez unieważnienie jednej lub większej liczby ich własności ochrony dotyczących, przykładowo dostępności, integralności, autentyczności. Takie niekorzystne działanie może być czytane na przykład jako, "Intruz z prawami dostępu administratora lokalnego, prowadzi do unieważnienia dostępność dowodu interwencji." Sformułowanie całkowitego zagrożenia może być znalezione wewnątrz zakreskowanego obszaru na rysunku 1. Kompletny zbiór możliwych negatywnych działań wynikający z podstaw kombinatoryki, może być sprawdzony pod kątem spójności i możliwych powtórzeń. Końcowy krok implementacji ataku, składa się z niekorzystnych działań i wektora ataku, który będzie przypisany do indywidualnego wpływu o punktacji od 1 do 5. Odtąd przyjmuje się, że wszystkie wymagania prawne są równie ważne i stosuje się dla nich najwyższy poziom punktacji (5). Niższa punktacja będzie wybrana jeśli atak odnosi się do pojedynczego pomiaru i jeśli atak ten może być później wykryty przez nadzór rynku.

TABELA 1

WYMAGANIA MID [1]. ODNIESIENIE DO OPROGRAMOWANIA I ICH FORMALIZACJA JAKO AKTYWA I WŁASNOŚCI OCHRONY. LICZBA W NAWIASACH PO KAŻDYM AKTYWIE (OD A1 DO A10) STANOWI UNIKALNY IDENTYFIKATOR.

|  |  |  |
| --- | --- | --- |
| **Wymaganie w MID [1] Aneks I** | **Aktywa** | **Własność ochrony** |
| 7.6 „Jeżeli przyrząd pomiarowy wyposażony jest w oprogramowanie realizujące inne funkcje, niż pomiarowe, oprogramowanie, które jest istotne dla charakterystyk metrologicznych, powinno być identyfikowalne i powinno być odporne na niedozwolony wpływ oprogramowania powiązanego.” | Identyfikacja software’u (A9) | dostępność, integralność |
| Niedopuszczalny wpływ na oprogramowanie (A5) | niedostępność |
| 8.1 „Charakterystyki pomiarowe przyrządu pomiarowego nie powinny podlegać wpływom jakiegokolwiek innego podłączonego urządzenia lub urządzenia, które komunikuje się zdalnie z przyrządem pomiarowym.” | Niedopuszczalny wpływ na oprogramowanie (A5) | niedostępność |
| 8.3 „Przyrząd powinien zapewnić identyfikację urządzenia.” | Prezentacja identyfikacji software’u (A10) | dostępność |
| 8.3 „Dowód ingerencji powinien być dostępny przez ustalony okres czasu.” | Ewidencja interwencji (A2) | dostępność, integralność |
| 8.4 „Dane pomiarowe, oprogramowanie istotne dla charakterystyk pomiarowych i ważne parametry metrologiczne przechowywane lub przekazywane powinny być odpowiednio zabezpieczone przed przypadkowym lub celowym zafałszowaniem.” | Mierzone dane (A3) | integralność, autentyczność |
| Software krytyczny dla charakterystyk metrologicznych (A1) | integralność, autentyczność |
| Istotne parametry metrologiczne | integralność, autentyczność |
| 10.1 „Identyfikacja wyników powinna występować na wyświetlaczu lub w postaci twardej kopii.” | Identyfikacja wyniku (A6) | dostępność, integralność |
| 10.2 „Identyfikacja wyniku powinna być jasna, jednoznaczna i uzupełniona przez oznaczenia i opisy informujące użytkownika o wartości wyniku.” | Oznaczenia i opisy (A7) uzupełniające identyfikację pomiaru | dostępność, integralność |
| 11.1 „Przyrząd pomiarowy inny niż narzędzie przyrządu pomiarowego powinno rejestrować w sposób ciągły wyniki pomiaru, opatrzone informacją, pozwalającą zidentyfikować daną transakcję, gdy: pomiar nie jest powtarzalny; i przyrząd pomiarowy jest zwykle przeznaczony do użytku pod nieobecność jednej ze stron transakcji.” | Zapis wyniku pomiaru (A8) | dostępność, integralność, autentyczność |

*B. Identyfikacja wektora ataku*

Drugi etap oceny ryzyka jest z pewnością najmniej sformalizowany. Zaczyna się on od wnikliwej analizy dokumentacji badanego przyrządu pomiarowego przedłożonej przez producenta. Proces ten pokazany jest w części środkowej Rysunku 1. Oceniający gromadzi możliwe wektory ataku, składające się z wykonywanych czynności, które umożliwiają atakującemu realizację zidentyfikowanych wcześniej zagrożeń. Stanowi to istotną różnicę wobec metody TISPAN wyjaśnionej w Rozdziale II. Pewne z tych wektorów ataku mogą być proste, jak próby dostępu na wyższym poziomie poprzez wprowadzane z klawiatury znaków hasła. Inne mogą porównywać stronami złożone skrypty (XSS) atakując w połączeniu z przygotowaniem „root kit” obejmującym całe urządzenie i następnie instalujące na urządzeniu nieuprawnione oprogramowanie. Jeden relatywnie prosty wektor ataku z tej kategorii wykonany jest w ataku odmowy obsługi (denial-of-service (DoS)) przyrządu pomiarowego połączonego z Internetem. W wielu przypadkach, atak taki spowoduje uzyskanie dowolnej liczby komunikatów wpisanych do dziennika kontroli, który podlega prawnej kontroli. Długość zapisu powinna być w swojej wielkości ograniczana, ponieważ wczesna interwencja może później nie być identyfikowalna jeśli log jest zalany ogromną ilością automatycznie generowanych błędów. Byłoby to bezpośrednim naruszeniem istotnych wymagań ustalonych w rozdziale III.

1. *Obliczanie punktów prawdopodobieństwa i ryzyka*

Jeśli w jednym lub większej liczbie wektorów ataku zidentyfikowane zostaną szkodliwe działania, pozostaje obliczyć prawdopodobieństwo, z którym zaimplementowany został aktualny atak, patrz dolna część Rysunek 1. Podobne działanie jest szczegółowo opisane w analizie wrażliwości (klasa AVA\_VAN) w [12]. Tam, dla pewnych ataków, oceniający szacuje odporność produktu IT (TOE w języku CC). Obliczenia w [12] przeprowadzone są na podstawie pięciu punktów opisujących źródła wymagane do przeprowadzenia ataku:

* Czas (0-19 punktów)
* Rzeczoznawstwo (0-8 punktów)
* Wiedza o TOE (0-11 punktów)
* Okno możliwości (0-10 punktów)
* Wyposażenie (0-9 punktów)

Punktacja upływu czasu reprezentuje zawartość czasu potrzebnego agresorowi do implementacji określonego ataku. Punktacja równa 0 oznacza zazwyczaj pracę krótszą niż dzień. Potrzeba pracy trwającej mniej niż tydzień daje punktację 1, natomiast 19 reprezentuje okres czasu przybliżany na więcej niż pół roku pracy. W Rozdziale V pokazanych zostanie więcej przykładów. Tabela ze szczegółami wszystkich pięciu kryteriów punktacji i dodatkowe wyjaśnienia dla wybranych kryteriów znaleźć można w [12, p. 429].

Logarytmiczny przyrost punktacji spowodowany jest tym, że każdy dodatkowy punkt przypisany atakowi, wywołuje znacząco większą trudność implementacji.

TABELA II

OBLICZENIA OPORU TOE. TRZECIA KOLUMNA MAPUJE OPÓR TOE DO ODPOWIEDNIEJ PUNKTACJI PRAWDOPODOBIEŃSTWA I NIE JEST CZĘŚCIĄ ORYGINALNEJ TABELI DANEJ W [12]

|  |  |  |
| --- | --- | --- |
| **Suma punktów** | **Opór TOE** | **Punkty prawdopodobieństwa** |
| 0 - 9 | Brak wpływu | 5 |
| 10 - 13 | Podstawowy | 4 |
| 14 - 19 | Podstawowy rozszerzony | 3 |
| 20 - 24 | Podwyższony | 2 |
| >24 | Wysoki | 1 |

Oznacza to także, że punkt jest łatwiejszy do powielenia ponieważ ewaluatory nagle rosną z estymacją czasów ataku o tej samej wielkości nawet jeśli aktualny czas jest nieco różny. W drugiej kategorii (rzeczoznawstwo), mogą być przypisane punkty między 0 i 8, gdzie 0 reprezentuje możliwości laika i punkty 8 występują są, gdy agresor musi być ekspertem w więcej niż jednej dziedzinie. Trzecia kategoria odnosi się do wymagań wiedzy koncentrującej się na atakowanym urządzeniu. I znowu, punkt 0 występuje jest jeśli wymagana jest powszechnie znana wiedza, jak łatwo osiągalne informacje z sieci, punkt 3 reprezentuje wiedzę restrykcyjną, która może być znaleziona w dokumentacji użytkownika. Maksimum 11 punktów powinna stanowić wewnętrzna krytyczna informacja dostępna pracownikom produkcji. Jednym bardzo istotnym kryterium jest okno możliwości dostępne dla określonego agresora. W przypadku nieograniczonego dostępu, co mogłoby być możliwe dla urządzeń połączonych z Internetem, dane są punkty 0, gdzie punkt 1 oznacza łatwy dostęp. Trudnemu dostępowi należy przypisać 10 punktów. W idealnym przypadku, gdy dostęp nie jest możliwy, nie występuje żadna punktacja i odpowiedni wektor ataku powinien być usunięty z listy kandydatów. W tym punkcie występuje prosty sposób włączenia do punktacji zagrożeń wynikających z implementacji motywacji agresorów. Jeśli agresorowi brak motywacji do implementacji zagrożenia nawet jeśli byłby on zdolny do realizacji wektora ataku, odpowiednie zagrożenie powinno być usunięte z listy.

Jeśli przypisano punkty dla pięciu wymienionych kategorii, obliczana jest całkowita suma punktów. Podczas obliczeń CC pobierany jest tak zwany opór TOE, jak pokazuje tabela II. Zakres punktacji pomiędzy 10 i 13 mógłby przykładowo demonstrować podstawowy opór stawiany agresorom, podczas gdy punktacja powyżej 24 wskazuje wysoki opór. W kontekście CC, opór stawiany agresorowi mogłaby być zatem wykorzystany do sprawdzenia poprawności wybranego uzasadnionego poziomu zaufania (evaluation assurance level (EAL)). Tutaj jednak, mapowany jest udział oporu do prawdopodobieństwa pomiędzy 1 i 5, gdzie 5 reprezentuje wysokie prawdopodobieństwo wystąpienia ataku i 1 stan, kiedy atak jest bardzo mało prawdopodobny. Mapowanie oporu TOE do punktów prawdopodobieństwa pokazane jest w Tabeli II.

Obliczenia oszacowania ryzyka skojarzonego z zagrożeniem w konsekwencji składa się z iloczynu punktów wpływu (pomiędzy 1 i 5) danego zagrożenia z punktacją prawdopodobieństwa najbardziej prawdopodobnego wektora ataku, który mógłby realizować zagrożenie:

Wynik ryzyka = punkty wpływu \* punkty prawdopodobieństwa / 5 (1)

Dzieląc punkty wpływu przez 5 zapewnia się, że punktacja ryzyka wystepuje w zakresie pomiędzy 1 i 5. Jak zostało pokazane w obliczeniach eksperymentalnych, punkty ryzyka łatwo mogą być wykorzystane do stopniowania ryzyka skojarzonego z pojedynczym przyrządem lub nawet do porównywania różnych przyrządów i ich ryzyka ze sobą.

V. EKSPERYMENTALNE OBLICZENIA I PORÓWNANIE Z INNYMI METODAMI

*A. Wilgotnościomierz ziarna*

Pierwszym przyrządem pomiarowym, który został sprawdzony podczas obliczeń zaproponowanej softwarowej metody oceny ryzyka jest analizator wilgotności ziarna. Urządzenie takie zazwyczaj stosuje się do niewielkiej ilości ziaren i w granicach próbki oblicza poziom wilgotności, rzucając na nie światło podczerwone i obserwując pochłonięte spektrum długości fal. Względna wilgotność jest ekonomicznie ważna ponieważ ma ona znaczący wpływ na ocenę ziarna. W tym przypadku przyrząd pomiarowy jest autonomiczną jednostką, która jest zamknięta fizycznie z wyjątkiem ekranu dotykowego, wlotu próbek jak również portu szeregowego USB. Systemem operacyjnym są Windowsy CE. Poprzez ekran dotykowy mogą być wybrane pewne typy ziaren, który także jest wykorzystany do rozpoczęcia procesu pomiaru i pokazuje aktualny i poprzednie wyniki. Ponadto urządzenie zawiera tzw. dziennik kontroli, w którym zapisywane są zmiany zarówno software’u jak i odpowiednich parametrów pomiarowych. Jeśli do jednostki dołączona jest pusta pamięć USB, będzie ona zapisywać na nośniku wszystkie dostępne wyniki razem z odpowiednimi danymi i czasem pomiaru . Proces pomiarowy można również uruchomić za pośrednictwem portu szeregowego, który wykorzystuje własny protokół. Przez ten protokół mogą również być odczytane wyniki pomiaru. Dostęp do istotnych parametrów systemu i do systemu operacyjnego jest chroniony 6-io znakowym hasłem. Schemat systemu na wysokim poziomie ogólności można znaleźć na Rysunku 2.

Opierając się na architekturze systemu i dokumentacji dostarczonej przez producenta może być skompilowana prawdopodobna lista wektorów ataku. Następująca lista jest właśnie krótkim fragmentem listy i jest tutaj użyta dla celów poglądowych:

* **A\_PASSWORD**: Osoba atakująca osiągnie dostęp do hasła administratora i próbuje wszystkich 6-cio cyfrowych kombinacji.
* **A-SW\_REPLACE**: Osoba atakująca pozyska hasło administracyjne i zamieni legalny software.
* **A\_INT\_SERIAL**: Osoba atakująca wykorzystuje lukę w zastrzeżonym protokole szeregowym, co jest powodem awarii urządzenia.
* **A\_INT\_SERIAL\_VALUE**: Osoba atakująca wykorzystuje lukę i własnym protokołem manipuluje wartościami mierzonymi przerywając pomiar.
* **A\_INT\_USB**: Osoba atakująca zdołała zainstalować na przyrządzie pomiarowym złośliwy kod, wyłączając ochronę użytkownika portu USB.

Dla każdego, wyżej opisanego zagrożenia, ewaluator musi teraz przeglądać listę wektorów ataku i wybrać te, które mogą realizować zagrożenie. W pewnych przypadkach konieczna może być kombinacja wektorów ataku. Fragment kompletnego odwzorowania pomiędzy scenariuszem zagrożeń i wektorem ataków może być znaleziony w tabeli III. Każde zagrożenie może być zatem ocenione indywidualnie. Zarówno wynik punktacji dla każdego aspektu i jego znaczenie są również dostarczone w tabeli. Tutaj pierwszym zagrożeniem (T1) jest zamiana przez atakującego właściwego legalnego oprogramowania. Ponieważ jedyną osobą z odpowiednim dostępem do przyrządu pomiarowego jest operator urządzenia, przyjmuje się, że jest on także osobą atakującą. To oczywiście ma wpływ na przypisanie zgromadzonych punktów (patrz tabela III). Aby zrealizować T1, atakujący po pierwsze pobiera hasło z systemu operacyjnego. Dodatkowo, oprogramowanie musi być tak napisane, że naśladuje spodziewane zachowanie bez powstania podejrzenia u klienta. Opracowanie takiego oprogramowania jest uważane za bardzo złożone, nadając mu ocenę czasu realizacji większą niż pół roku i towarzyszy temu wynik punktacji 19. Ponadto atakujący musi być ekspertem w dziedzinie opracowania software’u lub mieć dostęp do kogoś, kto ma takie umiejętności. Dlatego wynik ekspertyzy wynosi 6. Wymagana jest także wiedza restrykcyjna na temat zachowania systemu i jego komponentów. Wreszcie, właściciel przyrządu mając do niego nieograniczony dostęp i do napisania software’u nie ma specjalistycznego wyposażenia oprócz podstawowego, wymaganego na PC. Wynik sumy w tej sytuacji to 29, który w kontekście CC jest na tyle wysoki, że prawdopodobieństwo praktycznie nie występuje. Tabela II w związku z tym przypisuje temu zagrożeniu najniższą punktację prawdopodobieństwu. Następne zagrożenia od T2 do T5 są obliczane w ten sam sposób. Zagrożenie T5 ma ocenę prawdopodobieństwa 2, która jest identyczna z zagrożeniami T3 i T4. Najmniejsza jednak skala ryzyka to tylko 1 ponieważ T5 wpłynie tylko na jeden wynik pomiaru i dla tego ma stosunkowo niewielkie znaczenie. Dla wszystkich innych zagrożeń nie ma różnicy między punktami ryzyka i prawdopodobieństwa, są one sklasyfikowane na najwyższym możliwym poziomie 5.

*B. Pompa paliwowa*

Drugi przyrząd pomiarowy, który został obliczony zgodnie z nowym zaproponowanym tutaj schematem jest kalkulator jednostki pompa paliwowa. Urządzenie komunikuje się z otoczeniem poprzez układ punkt-sprzedaży ((point-of-sales ) POS) i czyta dane z szeregu przepływomierzy tłokowych. Jako system operacyjny użyto Linux’a. Wyniki pomiarów są wyświetlane lokalnie na siedmio-segmentowym wyświetlaczu i są również przesyłane po sieci LAN do urządzenia POS. Komunikacja z urządzeniem POS jest jednokierunkowa. Parametry, które wpływają na zachowanie się systemu metrologicznego i systemu operacyjnego mogą być zmienne i dostępne, gdy pamięć USB z 32 bitowym kluczem jest podłączona do urządzenia. Zwykle klucz jest w posiadaniu uprawnionego inspektora. Dodatkowo urządzenie posiada serwer WWW, który jest dostępny w Internecie. Poprzez interfejs WWW, może być sprawdzony status urządzenia i ustawiane parametry.

Uproszczony schemat przyrządu pomiarowego i jego otoczenia można znaleźć na rysunku 3. Lista możliwych scenariuszy ataku noże być zidentyfikowana na podstawie dokumentacji dostarczonej przez producenta. Najprostszy sposób uzyskania wektorów ataku to skoncentrowanie się na dostępnych interfejsach z otoczenia. Obejmują one port USB i komunikację z urządzeniem POS jak również interfejs WEB. Komunikacja z urządzeniem POS jest fizycznie zamknięta, ponieważ jest również pod kontrolą prawną. Port USB jest łatwo dostępny dla właściciela pompy, a interfejs internetowy jest swobodnie dostępny dla każdego posiadacza adresu IP. Serwer WWW w kwestii, jak powszechnie używane są produkty IT, ma kilka wpisów w publicznej bazie CVE [15], która jest używana przez MITRE, spółkę non-profit działającej w wielu centrach badawczo rozwojowych finansowanych przez rząd US.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Zagrożenie** | **Opis** | **Wpływ** | **Wektor ataku** | **Czas trwania** | **Rzeczoznawstwo** | **Wiedza TOE** | **Okno możliwości** | **Wyposażenie** | **Suma** | **Punkty** | **Ryzyko** |
| T1 | Lokalny administrator (S1) sprawdza integralność lub autentyczność oprogramowania metrologicznego (O1). | 5 | A\_SW\_RE\_PLACE | (>180d) 19 | (ekspert) 6 | (restrykcyjna) 3 | (nieograniczone) 0 | (standardowe) 0 | 28 | 1 | 1 |
| T2 | Lokalny administrator (S1) sprawdza dostępność do ewidencji interwencji (A2). | 5 | A\_INT\_SERIAL | (>30d) 4 | (biegły) 3 | (wrażliwa) 7 | (nieograniczony) 0 | (specjalizowany) 4 | 18 | 3 | 3 |
| T3 | Lokalny administrator (S1) sprawdza integralność parametrów metrologicznych (A4). | 5 | A\_INT\_SERIAL\_VALUE | (>60d) 7 | (ekspert) 6 | (Wrażliwa) 7 | (nieograniczone) 0 | (specjalizowany) 4 | 24 | 2 | 2 |
| T4 | Lokalny administrator sprawdza dostępność do ewidencji interwencji (A2) poprzez usunięcie ewidencji | 5 | A\_PASSWORD | (>180) 19 | (laik) 0 | (restrykcyjna) 3 | (nieograniczone) 0 | (standardowe) 0 | 22 | 2 | 2 |
| T5 | Lokalny administrator (S2) sprawdza integralność, autentyczność lub dostępność wyniku pomiaru (A8). | 2 | A\_INT\_USB | (>60d) 7 | (ekspert) 6 | (restrykcyjna) 3 | (nieograniczona) 0 | (specjalizowana) 4 | 20 | 2 | 1 |

Baza zawiera obszerną listę znanych luk praktycznie wszystkich publicznie dostępnych programów. Krótki fragment listy możliwych kierunków ataku tutaj będzie przedstawiony:

* **A\_USB\_SCRIPT**: Atakujący podrabia klucz autoryzacji na USB mając w ten sposób dostęp do systemu operacyjnego.
* **A\_WEB\_XSS**: Atakujący wykorzystuje CVE-2011-4273 dla ataku XSS aby wykonać arbitralnie kod JavaScript na serwerze web i w konsekwencji pobrać „root kit” systemu.
* **A\_WEB\_DOS**: Atakujący wykorzystuje CVE-2009-5111, CVE-2003-1568 lub CVE-2002-2429, wykonując atak DoS poprzez cząstkowe żądania http.
* **A\_WEB\_SOCKED**: atakujący wykonuje złośliwy kod podczas ustanawiania połączenia wykorzystując CVE-2002-2431.

Jak w poprzednim przykładzie, wszystkie znane zagrożenia są sprawdzane iteracyjnie. Dla każdego z nich, oceniający musi zdecydować, czy istnieją wektory ataków, które mogą być użyte do realizacji odpowiedniego zagrożenia. Następnie znowu obliczana jest, kombinacja zagrożenia i wektora ataku używając punktacji CC. Również tutaj, zagrożenie T1 składa się wymiany odpowiedniego legalnego oprogramowania w celu uzyskania dostępu do systemu operacyjnego. Ponieważ hasło zostało wprowadzone poprzez port USB, istnieje możliwość wykonania zautomatyzowanego ataku „brutalnej siły” na dane autentykacyjne. Wymaga to jednak znacznych zasobów. Ponadto, napisanie wymienionego oprogramowania wymaga pozorowania oryginału. I znowu, czas potrzebny na wdrożenie T1 jest duży, co prowadzi do punktacji 19. Ponadto, atakujący w kwestii umiejętności musi być ekspertem inżynierii oprogramowania (punktacja 6) ze szczegółową wiedzą o przyrządzie pomiarowym (punktacja 3). Jeżeli operator pompy oraz atakujący ma nieograniczony dostęp do urządzenia oczywistym jest odpowiednia punktacja 0. Ogólna suma 29 punktów jest tak wysoka, że wynik prawdopodobieństwa jest znikomy, wynosi 1. Powinno to to być postrzegane w połączeniu z faktem, że wybrana kombinacja atakującego i możliwości są bardzo prawdopodobne w każdym przypadku.

O wiele bardziej prawdopodobny wydaje się atak na lokalny serwer WWW (patrz zagrożenia T2). Ponieważ eksploratory luk serwera mogą być pobrane z sieci, nie ma potrzeby angażowania znaczącego czasu (punktacja 4). Atakujący musi ponadto być ekspertem (punktacja 6) w dziedzinie inżynierii oprogramowania, aby prawidłowo zastosować eksploracje. Potrzebne są pewne szczegóły dotyczące przyrządu pomiarowego takie jak adres IP. Ponieważ atak oparty jest na sieci Web, dostęp jest praktycznie nieograniczony. Mając specjalizowany sprzęt taki jak platforma testowania ataków, wynikiem jest relatywnie niska punktacja 17. Rezultat ten jest średnim prawdopodobieństwem zagrożenia. Ocenę pozostałego zagrożenia rozwija się w podobny sposób. Wyniki oceny można znaleźć w tabeli IV. I znowu, ważne jest wspomnieć, że pewne zagrożenia (T5 i T6) maja niskie oceny ryzyka mimo średniego wyniku prawdopodobieństwa, ponieważ ich wpływ jest ograniczony do pojedynczego pomiaru w czasie.

1. *Porównanie z przewodnikiem WELMEC 5.3*

Przewodnik WELMEC 5.3 używa tych samych definicji ryzyka jak opracowanie dyskutowane tutaj: wpływ produktu i prawdopodobieństwo zdarzenia zagrożenia. Dodatkowo, przewodnik oblicza średni wpływ punktów opartych na implikacjach ekonomicznych, publicznej służby zdrowia, zaufaniu konsumentów i aspektach prawnych. Zagrożenie zidentyfikowane w rozdziale III, które wypływają z kategorii prawnej, powinny być także użyte w kontekście przewodnika. Jednak, prawdopodobieństwo estymacji w przewodniku WELMEC 5.3 wyraźnie ma na celu ”prawdopodobieństwo niezgodności“. Jest to adresowane zarówno do zachowania producenta i konsumenta jak i cyklu produkcyjnego przyrządu. Zagrożenie jest jasno skoncentrowane na producencie przyrządu. Niezamierzone, oparte na implementacji niedoskonałości przyrządu pomiarowego nie są objęte zakresem przewodnika WELMEC 5.3 ponieważ szczegóły techniczne uwzględniające komponenty przyrządu, nie są brane pod uwagę w ogóle. Zamiast tego, większy nacisk kładzie się na postrzeganie wymagań prawnych i statystyk dotyczących obszaru zagadnienia. Chociaż ten ostatni może dostarczyć pomocnych wskazówek i wcześniej może być stosowany do oceny ryzyka związanego z produktem. Przewodnik więc nie jest w stanie posłużyć do uzyskania porównywalnych wyników oceny.

1. *Porównanie z ISO/IEC 27005*

Najbardziej istotne różnice pomiędzy opracowaniem zaprezentowanym tutaj i w ISO/IEC 27005 [3] jest dodatkowo obliczane prawdopodobieństwo oparte na analizie luk CC i CEM. ISO/IEC 27005 wyraźnie stwierdza, że techniki szacowania prawdopodobieństwa powinny uwzględniać “motywację i możliwości i źródła dostępne dla możliwych agresorów, które są zmienne w czasie”. Zarówno motywacja i własności (uwzględniające wyposażenie, wymagane cechy i wiedzę) mogą jasno mapować CC-oparte prawdopodobnie na estymacji. Szczegółowe wyjaśnienia znajdują się w rozdziale IV. Nowe opracowanie ryzyka może więc by postrzegane jako realizacja praktyczna ISO/IEC 27007, która sama w sobie nie jest szczególnym sposobem obliczeń indywidualnego prawdopodobieństwa zagrożenia. Identyfikacja aktywów, jak opisano w rozdziale II, jest także jasno zgodna z ISO/IEC 27005, ponieważ wynika z tych samych trzech kroków opracowania identyfikacji ryzyka, estymacji ryzyka i obliczeń ryzyka. Jednak w normie można znaleźć wiele dodatkowych wskazówek dla dalszej poprawy metody:

* Motywacja lub źródła atakujących mogą zmieniać się w czasie, w taki sposób, że ocena ryzyka dla specjalnych przyrządów pomiarowych może być ponownie przeprowadzona po określonej przerwie czasu, aby utrzymywać ją na bieżąco.
* Nawet jeśli możliwy jest dla agresora dostęp do urządzenia, może on utracić motywację lub właściwości ochrony przed atakiem. Tak więc, każde zaimplementowane zagrożenie ze skojarzonym wektorem ataku powinno być sprawdzone ponownie z listą podobnych agresorów. Podobnie kombinacje własności i okna możliwości mogą być usunięte z tabeli obliczeń, ze skutkiem w jaśniej zdefiniowanym scenariuszu ryzyka.

VI POSUMOWANIE I PRZYSZŁA PRACA

Metoda oceny ryzyka dla przyrządów pomiarowych w metrologii prawnej tutaj opisana wynika z przewodników ISO/IEC 18045 [12] skąd wyprowadzono wielkości punktacji prawdopodobieństwa dla niektórych zagrożeń. W celu uzyskania bardziej obiektywnego procesu obliczeniowego, sformalizowane zostały wymagania prawne dla przyrządów pomiarowych jak wynika dalej z [1], z listy aktywów podlegających ochronie i odpowiadających im własności ochrony. W celu pokazania możliwości podejścia, zbadano dwa rzeczywiste przykłady przyrządów pomiarowych uzyskując wyniki, które mogą być wykorzystane przez producentów jako informacja zwrotna do projektowania i fazy produkcji. Nawet jeśli wszystkie aplikacje scenariuszy tutaj dyskutowanych pochodzą z obszaru metrologii prawnej, opracowanie może być interesujące dla ewaluatorów programowych w ogóle. Formalizacja aktywów i wymagań bezpieczeństwa może, oczywiście być zaadoptowana dla dopasowania się do innych wymogów prawnych lub konstrukcyjnych pochodzących częściowo z MID. Następnie może być zastosowany schemat rozwoju w ten sam sposób jak zademonstrowano tutaj. Dwa przykłady wykorzystane do demonstracji rozwiązania pokazały, że schemat może rzeczywiście dostarczyć znaczących wyników opartych na informacjach dostępnych dla Jednostki Notyfikującej podczas oceny projektu przez producenta. Jeśli dostępny jest także kod źródłowy, metoda z [7] może być zastosowana do późniejszego sprawdzenia określonego scenariusza ryzyka. Nawet bez dodatkowych informacji określona jest liczba kroków, które mogą być przeprowadzone dla poprawy zaproponowanego opracowania:

W pierwszym kroku, różni ewaluatorzy będą pytani o ogólną ocenę przyrządu pomiarowego w testach polowych. W tym celu, podejście to jest testowane w podgrupie roboczej WELMEC Working Group 7 „Software”. Podczas testów badana jest powtarzalność wyników w warunkach rzeczywistych. Po drugie, lepiej opracowany model agresora może być rozprowadzany aby włączyć więcej informacji o stosowanych polach zagrożeń w przyrządach pomiarowych. W kroku tym, mogłaby także być dodana motywacja pewnych agresorów jako odrębnych komponentów obliczeń. Zmiana taka będzie również wymagać identyfikacji wyników punktowych w CC i tym samym będzie wymagać ostrożnych korekt. Po drugie, lepiej rozwinięte modele atakującego będą zawierać więcej informacji na temat użycia pól zagrożeń w przyrządzie pomiarowym wykorzystywanych w ocenie. Na tym etapie, motywacja niektórych atakujących może także być dołączona jako kolejny składnik obliczeń. Zmiana taka wymagałaby modyfikacji punktacji w CC i tym samym stanowiłaby bardzo wrażliwą zmianę.

LITERATURA

[1] “Directive 2014/32/EU of the European Parliament and of the Council of

26 February 2014 on the harmonisation of the laws of the Member States

relating to the making available on the market of measuring instruments,”

European Union, Council of the European Union ; European Parliament,

Directive, February 2014.

[2] D. Peters, U. Grottker, F. Thiel, M. Peter, and J.-P. Seifert, “Achieving

software security for measuring instruments under legal control,” in

Proceedings of the Federated Conference on Computer Science and

Information Systems, vol. 3, Warsaw Poland, September 2014, pp. 123–

130, DOI: 10.15439/2014F460.

[3] “ISO/IEC 27005:2011(e) Information technology - Security techniques

- Information security risk management,” International Organization for

Standardization, Geneva, CH, Standard, June 2011.

[4] G. Geiger, “Ict Security Risk Management: Economic Perspectives,” in

Proceedings of the Federated Conference on Computer Science and Information

Systems, vol. 3, 2014, pp. 119–122, DOI: 10.15439/2014F439.

[5] “Regulation (EC) No 765/2008 of the European Parliament and of the

Council of 9 July 2008 setting out the requirements for accreditation

and market surveillance relating to the marketing of products,” European

Union, Council of the European Union ; European Parliament,

Regulation, July 2008.

[6] “WELMEC 5.3 Risk Assessment Guide for Market Surveillance: Weigh

and Measuring Instrument,” European cooperation in legal metrology,

WELMEC Secretariat, Ljubljana, Standard, May 2011.

[7] A. van Deursen and T. Kuipers, “Source-based software risk assessment,”

in Proceedings of the IEEE International Conference on

Software Maintenance. IEEE, September 2003, pp. 385–388, DOI:

10.1109/ICSM.2003.1235448.

[8] S.-W. Foo and A. Muruganantham, “Software risk assessment model,”

in Proceedings of the IEEE International Conference on Management

of Innovation and Technology, vol. 2. IEEE, November 2000, pp. 536–

544, DOI: 10.1109/ICMIT.2000.916747.

[9] N. Greif and G. Parkin, “An international harmonised measurement

software guide: the need and the concept,” in Proceedings of the IMEKO

World Congress Fundamental and Applied Metrology, Lisbon, Portugal,

September 2009, pp. 2440–2443.

[10] M. Sadiq, M. K. I. Rahmani, M. W. Ahmad, and S. Jung, “Software risk

assessment and evaluation process (sraep) using model based approach,”

in Proceedings of the IEEE International Conference on Networking

and Information Technology. IEEE, June 2010, pp. 171–177, DOI:

10.1109/ICNIT.2010.5508535.

[11] “ISO/IEC 15408:2012 Common Criteria for Information Technology

Security Evaluation,” International Organization for Standardization,

Geneva, CH, Standard, September 2012, Version 3.1 Revision 4.

[12] “ISO/IEC 18045:2012 Common Methodology for Information Technology

Security Evaluation,” International Organization for Standardization,

Geneva, CH, Standard, September 2012, Version 3.1 Revision 4.

[13] “ETSI TS 102 165-1 Telecommunications and Internet converged Services

and Protocols for Advanced Networking; Methods and protocols;

Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,”

European Telecommunications Standards Institute, Sophia Antipolis

Cedex, FR, Standard, March 2011, v4.2.3.

[14] “WELMEC 7.2 Software Guide,” European cooperation in legal metrology,

WELMEC Secretariat, Delft, Standard, March 2012.

[15] “CVE - Common Vulnerabilities and Exposures,” https://cve.mitre.org/,

Accessed 04|17|2015.