Ireneusz J. JÓŹWIAK [1], Artur SZLESZYŃSKI [2]
[1] INSTYTUT INFORMATYKI, WYDZIAŁ INFORMATYKI I ZARZĄDZANIA, POLITECHNIKA WROCŁAWSKA, ul. Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
[2] KADRA INŻYNIERII SYSTEMÓW, WYDZIAŁ ZARZĄDZANIA, WYŻSZA SZKOŁA OFICERSKA WOJSK LĄDOWYCH IM. GEN. T. KOŚCIUSZKI, ul. Czajkowskiego 109, 51-150 Wrocław

Ocena wpływu incydentów na poziom bezpieczeństwa zasobów informacyjnych metodą modelowania zagrożeń

Dr hab. inż. Ireneusz J. JÓŹWIAK

Profesor w Instytucie Informatyki, Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej. Kierownik Zakładu Bezpieczeństwa i Niezawodności Systemów Informatycznych. W pracy naukowej koncentruje się na zagadnieniach bezpieczeństwa i niezawodności systemów informatycznych.

e-mail: Ireneusz.jozwiak@pwr.wroc.pl

Mgr inż. Artur SZLESZYŃSKI

Wykładowca w Katedrze Inżynierii Systemów Wydziału Zarządzania Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. Tadeusza KOŚCIUSZKI. W pracy naukowej koncentruje się na zagadnieniach bezpieczeństwa, wydajności oraz niezawodności systemów teleinformatycznych.

e-mail: a.szleszynski@wso.wroc.pl

Streszczenie

W artykule opisano zastosowanie metody modelowania zagrożeń dla potrzeb oceny poziomu bezpieczeństwa systemów informatycznych. Przedstawiono modyfikację metody bazującą na wykorzystaniu diagramów sekwencji do oceny zagrożeń w opracowywanym systemie informatycznym. Na podstawie przykładowego systemu teleinformatycznego (STI) zidentyfikowano wybrane incydenty, a następnie przeprowadzono analizę ich wpływu na STI. Autorzy przedstawili wykorzystanie metody modelowania zagrożeń rozbudowując ją o ocenę skumulowanych negatywnych skutków incydentu do ewaluacji poziomu bezpieczeństwa zasobów informacyjnych. Następnie opisano próbę połączenia uzyskanych wyników analizy ze zmianą atrybutów bezpieczeństwa informacji znajdujących się wewnątrz STI.

Słowa kluczowe: bezpieczeństwo systemu teleinformatycznego, metoda modelowania zagrożeń.

Assessment of incident influence on information assets security by Threat Modelling Method

Abstract

The paper presents the use of the Threat Modelling Method (TMM) for assessing the incident influence on information assets security. The authors describe a modification of the first solution version which was used to identify ICT vital elements of the created software. The initial version of the TMM method is described in references. Each ICT system has entry points that are the connection between the software system and the outside environment. They are responsible for an interaction with the users and other systems or devices. The modification can be especially used for analysis of the software part of the ICT system. The process of analysis employs sequence diagrams to find potential vulnerabilities which may be exploited by an intruder. Then the authors show the use of the graph as an ICT system substitute. This technique enables identification of the system crucial element or elements. The subject of examination is the incidence between the graph vertexes. Each of them represent one of the element of the evaluated ICT system. The dependencies between vertexes and arcs expressed in vertex's degree help to discover which of the elements is crucial for proper ICT system work. A crucial element of the system will generate the largest losses when the incident occurs. The authors propose measurement of consequence of incident occurrence for each element (formula (2)). Formula (3) presents an aggregated risk connected with the incident occurrence and its negative results. The calculation of the aggregated risk enables preparing the ranking of possible incidents and their consequences. The ranking helps to discover which incident in which elements is the most dangerous for the evaluated system work. The method disadvantage is lack of a simple relation between the ICT system element, incident, message and its consequence (formula (1)). This is because the method is adopted from the analysis of software systems to the analysis more complex ICT systems. This kind of systems (ICT) consists of software, telecommunication equipment and computer devices. All of them can be affected by the incident and all of them can be the source of disturbance in ICT system operation.

Keywords: ICT security, Threat Modelling Method.

1. Wprowadzenie

Ocena zagrożeń oraz poziomu bezpieczeństwa zasobów informacyjnych jest elementem procesu tworzenia systemu zabezpieczeń. W literaturze przedmiotu można znaleźć kilka metod umożliwiających ocenę zagrożeń dla zasobów informacyjnych organizacji. Konieczność udostępniania zasobów informacyjnych odbiorcom, znajdującym się w znacznej odległości od źródła informacji, wymaga zastosowania środków ochrony umożliwiających właściwą ochronę przesyłanych wiadomości [1, 5].

Metoda modelowania zagrożeń została opracowana w firmie Microsoft do oceny poziomu bezpieczeństwa tworzonych produktów programistycznych [8]. Celem metody jest identyfikacja możliwych scenariuszy ataków, przeprowadzanych przez intruzów, w celu przejęcia kontroli na programem lub zablokowania jego poprawnego działania [4, 8]. Działania te prowadzą do powstania strat, co z kolei zakłóca funkcjonowanie organizacji.

Organizacja chcąc uniknąć strat związanych z utratą zasobów informacyjnych powinna utworzyć zespół zarządzający bezpieczeństwem informacji. Zalecenie do powołania takiego zespołu można znaleźć w normach np. w ISO/IEC – 27002. Również regulacje prawne odnoszące się do ochrony zasobów informacyjnych zalecają powołanie zespołu odpowiedzialnego za ochronę zasobów informacyjnych.

Od systemu zabezpieczeń zasobów informacyjnych organizacja oczekuje gwarancji, że straty nie wystąpią lub jeśli wystąpią to negatywne skutki dla funkcjonowania organizacji będą na poziomie akceptowalnym przez nią. Jest to podejście zgodne z prezentowanym w normie ISO/IEC – 15408 – 1 [2, 4, 5].

Chcąc dokonać oceny bezpieczeństwa zasobów informacyjnych będziemy posługiwać się pojęciem poziomu bezpieczeństwa. Założenie to wynika z definicji pojęcia bezpieczeństwo informacyjne prezentowanego w literaturze. Definicje te są ogólne i nieprecyzyjne, odwołują się do subiektywnego poczucia braku zagrożenia nie podając metody lub metod oceny jego poziomu [1, 5]. Podobne podejście do definicji bezpieczeństwa zasobów informacyjnych znajduje się w ustawodawstwie dotyczącym ochrony informacji [4]. Zatem poziom ochrony zasobów informacyjnych będzie rozumiany, jako zachowanie atrybutów bezpieczeństwa informacji na poziomie akceptowanym przez właściciela zasobów. Co oznacza, że zasoby informacyjne udostępniane są tylko uprawnionym użytkownikom, dla których są dostępne i niezmienione. Zabezpieczenia uniemożliwiają dostęp do informacji osobom lub organizacjom nieupoważnionym przez właściciela zasobu.

Ocena poziomu bezpieczeństwa zasobów informacyjnych nie powinna polegać na subiektywnej ocenie osoby wykonującej ewaluację będącej jednocześnie odpowiedzialną za bezpieczeństwo rozwiązania. Ocena taka ma miejsce w przypadku nie wykonywania

audytu bezpieczeństwa przez instytucje zewnętrzne. Zatem ważnym elementem jest opracowanie miar, które pozwolą na weryfikację rzeczywistego poziomu ochrony zasobów informacyjnych. Zadanie to nie jest łatwe gdyż systemy teleinformatyczne nie są do siebie podobne [9]. Wszystkie eksploatowane rozwiązania noszą indywidualne cechy ich twórców przez to próba bezpośredniego porównania dwóch różnych rozwiązań jest trudna lub niemożliwa [4, 9]. Od procedury diagnostycznej oczekuje się powtarzalności uzyskanych wyników oceny bez względu na to kto ją przeprowadza [9].

2. Aktualny stan wiedzy i geneza problemu

Mierząc poziom bezpieczeństwa zasobów informacyjnych znajdujących się wewnątrz systemu teleinformatycznego (STI) należy określić podmiot badania. Bezpieczeństwo zasobów informacyjnych będzie zależeć od bezpieczeństwa procesów gromadzenia, przetwarzania i przesyłania danych oraz od poziomu zabezpieczenia urządzeń wykonujących opisane czynności. Zatem, istotne jest określenie co będzie przedmiotem procedury diagnostycznej, czy diagnozie zostaną poddane bezpieczeństwo procesów czy bezpieczeństwo urządzeń wykorzystanych w wymienionych procesach [9].

Celem metod diagnostycznych, stosowanych do oceny poziomu bezpieczeństwa zasobów informacyjnych, jest wykrycie podatności znajdujących się wewnątrz systemów teleinformatycznych (STI), które mogą zostać wykorzystane przez atakującego [3, 4, 8, 10]. Działania te podejmowane są etapie tworzenia modelu nowego rozwiązania przed przystąpieniem do jego implementacji [3, 4, 5]. Im wcześniej zostaną wykryte punkty dostępu, które stwarzają potencjalne zagrożenie dla funkcjonowania STI tym szybciej można je usunąć [8, 10]. Model STI ma wskazać te miejsca w systemie, które będą zawierały podatności możliwe do wykorzystania przez atakującego. Identyfikacja tych miejsc (modułów, połączeń między systemowych, itp.) umożliwia opracowanie systemu zabezpieczeń. Każdy STI posiada punkty wejścia, które są interfejsem wykorzystanym do komunikacji pomiędzy użytkownikami a systemem [8]. Interakcje pomiędzy użytkownikami, a STI opisują scenariusze podzielone na dwie grupy: obsługiwane i nieobsługiwane [8]. Pierwsza grupa dotyczy interakcji przewidzianych przez twórców rozwiązania i prowadzących do uzyskania pożądanych skutków działania systemu. Druga grupa dotyczy interakcji, które nie zostały przewidziane przez twórców rozwiązania, a które mogą zostać wykorzystane przez atakującego do przejęcia kontroli na fragmentem lub całością STI [8].

W pracy autorstwa Wang L., Wong, E., Xu D. zaprezentowano wykorzystanie diagramów sekwencji do identyfikacja podatności w tworzonym systemie teleinformatycznym [10]. Wybór diagramu sekwencji wynikał z faktu, iż służy on do przedstawienia wymagań stawianych systemowi informatycznemu przez zamawiającego [10]. Autorzy pokazali związki przyczynowo skutkowe występujące pomiędzy zdarzeniami (identyfikowanymi, jako incydenty w bezpieczeństwie), a komunikatami powstającymi w ich wyniku. Do opisu związków występujących pomiędzy: obiektem, zdarzeniem i komunikatem, posłużyła zależność wyrażona przy pomocy wzoru (1). Zależność ta nazywana jest, przez autorów, modelem bezpieczeństwa systemu informatycznego

$$SD_{TM}(\mathrm{O},\mathrm{M},\mathrm{E}) \tag{1}$$

gdzie: SD_{TM} – model bezpieczeństwa systemu teleinformatycznego, O – obiekt, element systemu teleinformatycznego, M – komunikat wysyłany w wyniku wystąpienia zdarzenia identyfikowana, jako incydent w bezpieczeństwie, E – zdarzanie występujące w systemie teleinformatycznym, określane jako incydent w bezpieczeństwie systemu teleinformatycznego.

Znając sekwencję wiadomości możliwe jest określenie zależności czasowych zachodzących pomiędzy zdarzeniami występującymi w ocenianym systemie. Wiedza dotycząca sekwencji zdarzeń zachodzących w STI umożliwia przygotowanie działań chroniących je przed negatywnymi skutkami incydentów.

Ponieważ w artykule używane jest pojęcie incydentu w bezpieczeństwie informacyjnym STI to należy określić, jak jest ono definiowane. W literaturze przedmiotu można spotkać dwie definicje pojęcia incydentu w bezpieczeństwie informacyjnym. Pierwsza definicja pochodzi z normy PN ISO/IEC-17799, gdzie incydent w bezpieczeństwie informacyjnym określa się jako „*... pojedyncze zdarzenie lub serię niepożądanych zdarzeń lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji*" [3]. Inaczej pojęcie incydentu w bezpieczeństwie informacyjnym definiuje A. Białas, który stwierdza, iż „*incydent w bezpieczeństwie to niekorzystne zdarzenie związane z systemem teleinformatycznym, które według obowiązujących reguł lub zaleceń może być uznane za awarię, faktyczne lub domniemane naruszenie zasad ochrony informacji, lub prawa własności"* [1]. Do dalszych rozważań przyjęta zostanie definicja pierwsza.

Problemem, który należy rozwiązać jest zweryfikowanie możliwości wykorzystania metody modelowania zagrożeń do oceny wpływu incydentów na bezpieczeństwo systemu teleinformatycznego oraz na bezpieczeństwo znajdujących się w nim zasobów informacyjnych. Metoda modelowania zagrożeń była przewidziana do ewaluacji zagrożeń występujących w systemach informatycznych. Technika miała umożliwić identyfikację punktów wejścia[1] do systemu informatycznego, a następnie pozwolić ocenić wpływ zdarzenia[2] na bezpieczeństwo funkcjonowania elementów rozwiązania. W procedurze weryfikacji przydatności, metody modelowania zagrożeń do oceny wpływu incydentów na bezpieczeństwo zasobów informacyjnych, należy sprawdzić czy technika może być stosowana do modelowania zagrożeń dla elementów systemu, które nie są oprogramowaniem. Udzielenie odpowiedzi na przedstawiony problem jest ważne ponieważ system teleinformatyczny składa się z następujących elementów:

- oprogramowania (systemy operacyjne serwerów, stacji roboczych, oprogramowanie biznesowe i użytkowe, oprogramo wanie diagnostyczne, oprogramowanie chroniące sprzęt komputerowy, urządzania telekomunikacyjne oraz dane, itp.),
- sprzętu komputerowego (serwery, stacje robocze, skanery, drukarki, urządzania mobilne, sieciowe i przenośne nośniki danych, itp.),
- sprzęt telekomunikacyjny (media transmisyjne, urządzania lokalnych i rozległych sieci komputerowych, urządzania komunikacji indywidualnej np. modemy radiowe, itp.),
- użytkownicy.

Dalsza część rozważań pominie udział użytkowników w oddziaływaniu na bezpieczeństwo funkcjonowania systemu teleinformatycznego. Decyzja ta wynika z faktu, iż analiza motywacji do zachowań destrukcyjnych użytkownika wobec rozwiązania stanowi domenę psychologii lub psychiatrii, a nie znajduje się w domenie zainteresowań osób odpowiedzialnych za bezpieczne działanie rozwiązania. Administratorzy rozwiązania mają za zadanie zminimalizować możliwość wystąpienia destrukcyjnego działania użytkownika, a jeżeli taki incydent wystąpi to jego negatywne skutki winny być jak najmniejsze.

3. Analiza możliwości wykorzystania metody modelowania zagrożeń do oceny bezpieczeństwa zasobów informacyjnych

W pracy analizie poddany zostanie przykładowy systemem teleinformatyczny wykorzystany do prowadzenia wirtualnego sklepu. Zadaniem systemu teleinformatycznego obsługującego wirtualny sklep, jest:

– przyjmowanie zamówień składanych przy pomocy serwisu internetowego sklepu;

[1] Miejsca połączeń, opracowywanego oprogramowania, z otoczeniem zewnętrznym

[2] Zdarzenia traktowane, jako potencjalne zagrożenia dla funkcjonowania systemu informatycznego. Zdarzenie opisywane jest przy pomocy scenariuszy nieobsługiwanych czyli dotyczy zachowania rozwiązania niezgodnego z wymaganiami zamawiającego

– przygotowanie faktur oraz kontrola płatności,
– przygotowanie dokumentów podatkowych;
– obsługa wysyłki zamówień oraz zarządzanie towarami zgromadzonymi w magazynie.

Poziom bezpieczeństwa informacji określa oczekiwany, przez użytkowników rozwiązania, stan atrybutów bezpieczeństwa informacji rozmieszczonej w rożnych elementach infrastruktury technicznej. Oznacza to, że informacja będzie posiadała niezmienione wartości atrybutów bezpieczeństwa informacji[3]. Jeżeli wartości atrybutów bezpieczeństwa informacji, w wyniku wystąpienia incydentu, uległyby zmianie, różnice wartości powinny znajdować się w przyjętym zakresie. Zakres zmienności wartości atrybutów bezpieczeństwa informacji tworzy obszar akceptowanego poziomu bezpieczeństwa zasobów informacyjnych.

Chcąc określić poziom bezpieczeństwa należy ustalić oczekiwany stan poziomu ochrony zasobów informacyjnych oraz dopuszczalny zakres zmian wartości atrybutów bezpieczeństwa informacji. Dane te posłużą do weryfikacji trafności wyników oszacowania spodziewanego wpływu incydentu na wartość atrybutów bezpieczeństwa informacji.

Zbiór połączeń logicznych związany jest z identyfikacją przepływów danych pomiędzy elementami infrastruktury technicznej STI. Związki, pomiędzy elementami infrastruktury technicznej, mogą być przedstawiane przy pomocy grafów lub diagramów akcji. Wybór sposobu prezentacji połączeń logicznych pomiędzy elementami infrastruktury logicznej STI zależy od preferencji zespołu prowadzącego analizę.

Zaletą diagramów aktywności jest przedstawienie na jednym rysunku aktorów (klas uczestniczących w czynności) wraz z komunikatami wymienianymi pomiędzy nimi. Wadą diagramów aktywności jest nie przedstawienie, miejsca gdzie dana klasa jest umieszczona. Trudno zatem stwierdzić, jak incydent może oddziaływać na kilka elementów infrastruktury technicznej. W takim przypadku można użyć diagramów rozmieszczenia, które pokażą miejsce instalacji danej klasy. Dodatkowo można posłużyć się grafem, który będzie przedstawiał połączenia logiczne[4] pomiędzy elementami infrastruktury technicznej STI, które odpowiadają za przepływ danych między wymienionymi elementami (rys. 1). Użycie trzech typów diagramów rozbudowuje dokumentację wykorzystaną w procesie analizy.

Graf przedstawiający połączenia logiczne w STI umożliwia identyfikację węzłów o największych stopniach. Węzły posiadające najwyższe stopnie będą stanowiły newralgiczne elementy systemu teleinformatycznego. W przypadku grafu przedstawionego na rysunku 1, węzłem o najwyższym stopniu jest sieć telekomunikacyjna, którego stopień wynosi 10. Dzieje się tak ponieważ sieć telekomunikacyjna odpowiada za przesyłanie danych do pozostałych elementów STI. Zatem będzie ona stanowić punkt wejścia dla potencjalnego atakującego do penetracji systemu teleinformatycznego. Pozostałe elementy systemu teleinformatycznego (węzły grafu) posiadają te same stopnie wynoszące 2.

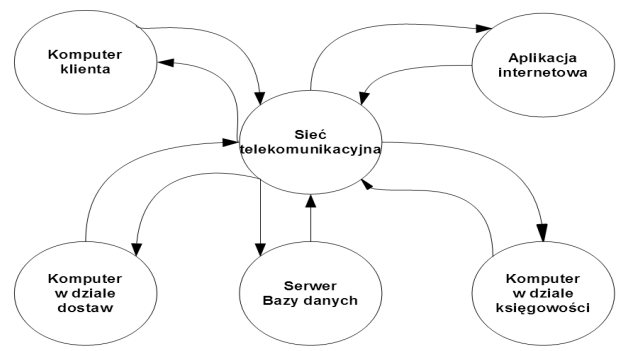
3.1. Implementacja metody modelowania zagrożeń do oceny incydentów w bezpieczeństwie STI

Zaprezentowane przykładowe rozwiązanie STI posiada następujące prawdopodobne podatności, które mogą stać się źródłem potencjalnych incydentów w funkcjonowaniu STI (tab. 1).

W przedstawionym rozwiązaniu obsługiwany scenariusz działania przedstawia się następująco, użytkownik STI nazywany klientem składa zamówienie wykorzystując swój komputer. Po zweryfikowaniu, przez aplikację internetową, nazwy użytkownika oraz jego hasła przystępuje On do złożenia zamówienia. Po złożeniu zamówienia następuje sprawdzenie liczby sztuk zamówionych towarów z liczbą dostępnych w magazynie. Jeżeli liczba zamówionych sztuk jest mniejsza od liczby dostępnych sztuk w magazynie, zamówienie zostaje przyjęte do realizacji. Po przyjęciu zamówienia do realizacji zostaje przygotowana paczka do wysyłki pocztowej oraz komplet dokumentów finansowych i księgowych.

Tab. 1. Zbiór możliwych incydentów w bezpieczeństwie informacyjnym dla modelu STI (źródło: opracowanie własne)
Tab. 1. A set of possible incidents in information security for a sample ICT system (source: the authors' own work)

Lp.	Opis incydentu	Elementy STI, na które wpływa incydent
1.	zmiana treści zamówienia składnego przez klienta, wykonana przez oprogramowanie złośliwe zainstalowane w komputerze klienta	komputer klienta, aplikacja internetowa, komputer w dziale dostaw, serwer bazy danych, komputer w dziale księgowości
2.	zwiększenie uprawnień przez atakującego i nieuprawniona modyfikacja danych w systemie	sieć telekomunikacyjna, serwer bazy danych
3.	uszkodzenie elementów sieci telekomunikacyjnej	sieć telekomunikacyjna, aplikacja internetowa, komputer w dziale dostaw, serwer bazy danych, komputer w dziale księgowości



Rys. 1. Przykładowy graf połączeń logicznych pomiędzy elementami infrastruktury technicznej STI (źródło: opracowanie własne)
Fig. 1. A sample graph presenting logical links between ICT system elements (source: the authors' own work)

Scenariusze nieobsługiwane przez STI wymienione są w tabeli 1. Jeżeli oprogramowanie złośliwe zmieni treść złożonego zamówienia wówczas dane te zostaną zapisane w bazie danych oraz przygotowane zostaną dokumenty finansowo-księgowe wymagające późniejszego skorygowania. Kolejny scenariusz nieobsługiwany związany jest z udanym atakiem na STI po stronie firmy. Jeżeli użytkownik może z powodzeniem uzyskać podwyższenie uprawnień, to z oznacza możliwość modyfikowania danych zapisanych w serwerze bazy danych. Sytuacja taka jest trudna do wykrycia, gdyż atakujący będzie weryfikowany przez podsystem zabezpieczeń, jako użytkownik posiadający wymagane uprawnienia.

Ostatni z wymienionych w tabeli 1 incydentów posiada największe negatywne skutki dla STI. Sieć telekomunikacyjna pełni rolę węzła łączącego wymienione elementy STI. Urządzenia wchodzące w jej skład znajdują się na terenie organizacji oraz poza nią. Elementy sieci telekomunikacyjnej znajdującej się poza terenem firmy mogą posłużyć do oddziaływania na STI. Dla przykładu uszkodzenie medium transmisyjnego łączącego lokalną sieć komputerową z rozległą siecią komputerową, jaką jest sieć Internet, będzie skutkować zatrzymaniem części procesów biznesowych związanych z komunikacją realizowaną przy pomocy sieci Internet. Incydent ten będzie oddziaływał na wymienione w tabeli 1 elementy STI uniemożliwiając wykonywanie czynności biznesowych. Opisany incydent może zostać wywołany celowo lub powstać w wyniku zdarzenia przypadkowego, jakim są np.

[3] Atrybuty bezpieczeństwa informacji przyjęto na podstawie normy ISO/IEC 17799:2007. Według normy informacja posiada następujące atrybuty bezpieczeństwa: poufność, integralność, dostępność.

[4] Przez połączenie logiczne rozumie się możliwość uzyskania dostępu do zasobów informacyjnych bez konieczności posiadania fizycznego połączenia pomiędzy elementami infrastruktury technicznej STI. Zob. ISO/IEC-17799:2007.

prace ziemne związane z modernizacją lub naprawą instalacji przesyłowych.

Wygenerowania komunikatu przez element systemu nie informuje o skutkach zdarzenia dla obiektu o_i oraz obiektu o_{i+1}. Chcąc uzyskać informację o możliwych negatywnych skutkach dla obiektu lub obiektów, powstałych w wyniku zdarzenia e_i, należy model rozszerzyć o atrybut opisujący skutki. Zatem skutek zdarzenia będzie zawierał informację obiekcie, w którym wystąpiło zdarzenie i o samym zdarzeniu. Ocenę skutków zdarzenia dla obiektu o_i można wyrazić przy pomocy wzoru (2) wykorzystywanego do oszacowania ryzyka, które w tym przypadku będzie traktowane jako skutek wystąpienia zdarzenia e_i w obiekcie o_i.

$$r_i(o_i,e_i) = mwst_{ei} \cdot k_i \tag{2}$$

gdzie: r_i – skutek wystąpienia zdarzenia e_i w obiekcie o_i, $mwst_{ei}$ – możliwość wystąpienia zdarzenia e_i w obiekcie o_i należącym do STI.$mwst_{ei} \in [0,1]$, k_i – negatywne konsekwencje wystąpienia zdarzenia e_i dla obiektu o_i.

Ponieważ wartość $mwst_{ei}$ dotyczy zdarzenia przyszłego, co do którego nie istnieje pewność, że wystąpi oraz jaka będzie częstość występowania, liczba ta określa miarę subiektywnego przekonania decydenta dotyczącą możliwości wystąpienia incydentu. Wiarygodniejszy sposób wyznaczenia wartości $mwst_{ei}$ realizowany jest przy pomocy metody delfickiej, wartość $mwst_{ei}$ zostanie wyznaczona na podstawie średniej z wyników podanych przez ekspertów.

Wybór wartości konsekwencji k_i można wykonać według zaleceń opisanych w metodzie ATAM [3, 4]. Wartość parametru k_i klasyfikowana jako niska może odpowiadać prostemu usprawnieniu uszkodzonego obiektu. Wartość średnia parametru będzie odpowiadać naprawie realizowanej w serwisie, zaś wartość wysoka będzie równoważna remontowi lub wymianie obiektu. Kryterium to może być odnoszone do kosztów związanych z naprawą (odtworzeniem zdatności) obiektu.

Znając wartość oczekiwaną skutku wystąpienia zdarzenia e_i dla obiektu o_i oraz ścieżkę propagacji zagrożenia można opracować ranking zdarzeń, które będą stanowiły największe potencjalne zagrożenie dla funkcjonowania STI. Ranking będzie wyznaczany na podstawie skumulowanych skutków dla poszczególnych elementów wchodzących w skład ścieżki propagacji zagrożeń. Skumulowany skutek obliczany jest według wzoru (3).

$$R_{szi} = \sum r_i(o_i,k_i) \tag{3}$$

gdzie: R_{szi} – skumulowany skutek (ryzyko) związany z wystąpieniem incydentu dla i-tej ścieżki propagacji zagrożenia, r_i, o_i, e_i – skutek wystąpienia zdarzenia e_i dla obiektu o_i wchodzącego w skład i-tej ścieżki propagacji zagrożenia.

Wyznaczone wartości skumulowanych skutków posłużą do przygotowania wektora, który zostanie uporządkowany od wartości największej do najmniejszej. Znając skumulowane skutki dla poszczególnych incydentów należy przystąpić do modyfikowania systemu zabezpieczeń. Możliwe jest wprowadzenie, do procesu analizy, preferencji dotyczącej ochrony wybranych elementów STI. Proces preferencji decyzyjnej wyrażany będzie przy pomocy wag przypisanych poszczególnym ścieżkom propagacji zagrożeń.

3.2. Ocena wpływu incydentów na bezpieczeństwo zasobów informacyjnych znajdujących się w STI

Określenie związków zachodzących pomiędzy incydentami, a zasobami informacyjnymi wymaga wskazania tych atrybutów bezpieczeństwa informacji [3, 4], których wartości mogą zostać zmienione w trakcie incydentu. Chcąc oszacować wpływ incydentu na wartość atrybutu bezpieczeństwa informacji należy ustalić wielkość liczbową danego atrybutu. W praktyce inżynierskiej powszechniej stosowanym rozwiązaniem jest przyjęcie miary jakościowej, która zostanie powiązana z wielkością liczbową wyznaczaną w trakcie dalszej ewaluacji rozwiązania [3, 4]. Rozwiązanie to wynika z uproszczenia procedury ewaluacyjnej, gdzie łatwiej jest stwierdzić, że zmiana wartości atrybutu bezpieczeństwa może być: duża, średnia lub mała niż stwierdzić że wyniesie ona np. 0,5 lub 4. Miara jakościowa pozwala na łatwe formułowanie subiektywnych ocen przez osoby wykonujące ocenę. Należy pamiętać, że bez pomiarów oceny te mogą nie oddawać rzeczywistej wielkości wpływu incydentu na atrybuty bezpieczeństwa informacji. Ocena jakościowa pozwala uniknąć problemu interpretacji miary numerycznej przez decydenta. Dla decydenta, wygodniejsza jest miara jakościowa niż miara numeryczna.

Określenie wartości liczbowej poszczególnych atrybutów bezpieczeństwa należy rozpocząć od ustalenia wartości początkowej dla danego atrybutu oraz oczekiwanego zakresu zmian. Kolejnym krokiem będzie utworzenie relacji z miarą jakością. Znajomość wielkości liczbowych atrybutów bezpieczeństwa oraz sposobów ich pomiaru umożliwi monitorowanie poziomu bezpieczeństwa zasobów informacyjnych znajdujących się wewnątrz STI.

Wyznaczenie wpływu incydentu na wartość zmian wartości atrybutów bezpieczeństwa informacji będzie polegało na oszacowaniu jego wielkości. Bezpośredni pomiar wielkości powstałych zmian wartości atrybutów bezpieczeństwa jest trudny, wynika on z braku metod, które umożliwiłyby w sposób jednoznaczny ocenienie zmian w wartościach atrybutów bezpieczeństwa informacji. Dla zobrazowania przedstawionej tezy można przedstawić następujący przykład czy uzyskanie dostępu do zasobu informacyjnego przez osobę nieupoważnioną jest jednoznaczne ze zmniejszeniem wartości atrybutu poufności tejże wiadomości? Takie stwierdzenie jest jedynie domniemaniem i do momentu kiedy informacja nie zostanie ujawniona można przyjmować, że wartość atrybutu poufności być może została zmniejszona, o jakąś wartość. Jak widać z przedstawionego przykładu oceny tego typu cechuje subiektywność, która wynika z wiedzy i doświadczenia osoby oceniającej[5]. Kwestia określenia zakresu zmian wartości atrybutów bezpieczeństwa informacji omawiane są obszerniej w pozycjach autorstwa I. Jóźwiaka oraz D. Kuchty [3, 4].

Ustalając zakres zmian wartości atrybutów bezpieczeństwa dla zasobów informacyjnych, należących do zbioru informacji wrażliwych[6], należy oszacować zakres zmian, jakie mogą powstać. Kolejną czynnością będzie ocena wpływu zmian, wartości atrybutów bezpieczeństwa informacji, na funkcjonowanie organizacji. Oceniając zakres zmian w połączeniu ze skutkiem wystąpienia incydentu dla każdego z obiektów zostaną zdefiniowane poziomy akceptowane i nieakceptowane zmian wartości atrybutów bezpieczeństwa. Sytuacje, w których wartości atrybutów bezpieczeństwa dla informacji należących do zbioru zasobów wrażliwych, będą skutkowały podjęciem działań mających na celu poprawę ich ochrony. Opracowane miary mogą być wyznaczone w sposób subiektywny, co będzie przedstawiać przewidywania wykonawcy lub wykonawców – oceny - dotyczących rozmiaru potencjalnych strat [4]. Ochroną przed taką sytuacją może być zastosowanie danych statystycznych dotyczących rodzaju oraz liczby incydentów lub zastosowanie metody delfickiej. Należy jednak pamiętać, że zagrożenia ewoluują i część danych może być bezużyteczna.

4. Wnioski

Zaproponowany model bezpieczeństwa systemu teleinformatycznego poprawnie opisuje element, którym jest oprogramowanie. Dzieje się tak ponieważ zmiany w strukturze danych wprowadzanych do programu mogą implikować generowanie komunikatów dotyczących nieoczekiwanego zachowania się programu[7].

[5] Ocenę tą można próbować zobiektywizować stosując np. metodę delficką polegającą na zebraniu, niezależnych ocen od grupy ekspertów, a następnie na ich uśrednieniu

[6] Pod pojęciem wrażliwych zasobów informacyjnych rozumie się te informacje które posiadają dla organizacji dużą wartość np. patenty, wynalazki, dane księgowe czy dane dotyczące realizowanych zamówień. Utrata lub uszkodzenie uniemożliwiające ich przetwarzanie lub wykorzystanie będzie powodem powstania znacznych strat dla organizacji

[7] Komunikaty te będą generowane przez program lub system operacyjny, w którym jest on uruchomiony

Problem pomiaru wpływu incydentów na bezpieczeństwo zasobów informacyjnych wymaga zdefiniowania stanów wyjściowych, związanych z ochroną zasobów informacyjnych, oraz zakresu zmian. Problem ten jest trudny w aplikacji gdyż wymaga wybrania tych elementów w informacji, które stanowią o jej wartości, a następnie należy przełożyć tą wiedzę na miary odpowiadających im atrybutów bezpieczeństwa. Stajemy tu przed problemem zdefiniowania jakości informacji oraz określenia wartości jej atrybutów.

Metoda pozwala wskazać ścieżki propagacji zagrożeń powstałych w trakcie incydentu. Po jej zmodyfikowaniu można oszacować skumulowane skutki dla każdej ze ścieżek propagacji zagrożeń, co stanowi standaryzowaną podstawę do podejmowania decyzji o modyfikacjach w systemie zabezpieczeń.

Mankamentem metody jest brak prostej relacji łączącej obiekt, zdarzenie, wiadomość oraz skumulowany rezultat z atrybutami bezpieczeństwa informacji. W trakcie dalszych badań zostanie podjęta próba opracowanie takiej relacji.

5. Literatura

[1] Białas A.: Bezpieczeństwo informacji i usług we współczesnej firmie, WNT, Warszawa 2006.

[2] Jóźwiak I.,J., Szleszyński A.: Ocena wpływu zabezpieczeń na poziom ochrony zasobów informacyjnych w systemach teleinformatycznych, Zeszyty Naukowe - Politechnika Śląska, z. 61 Organizacja i Zarządzanie, s. 181-190, 2012.

[3] Jóźwiak I.,J., Szleszyński A.: The Use of the Evaluation Method of Software System Architecture to Assess the Impacts on Information Security in Information and Communication Technology Systems, Journal of KONBIN 4(24) 2012. Safety and Reliability Systems, Publishing and Printing House of the Air Force Institute of Technology, Warszawa, Poland, pp. 59-70.

[4] Kuchta D., Szleszyński A., Witkowski M.: Metodyka opracowania scenariuszy przebiegu incydentów w bezpieczeństwie systemu, wykorzystywanych w zarządzaniu bezpieczeństwem informacji w wojskowych systemach teleinformatycznych, WSOWL, Wrocław 2012.

[5] Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa 2008.

[6] Liderman K.: Bezpieczeństwo informacyjne, PWN, Warszawa 2012.

[7] Narang M., Mehrotra M.: Security Issue – A Metrics Perspective, International Journal of Information Technology and Knowledge Management, July – December 2010, Vol. 2, No 2, pp. 567-571.

[8] Swiderski F., Window S.: Modelowanie zagrożeń, Promise, Warszawa 2005.

[9] Vaugh R.B., Heming R., Siraj A.: Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE Computer Society 2002.

[10] Wang L., Wong, E., Xu D.: A Threat Model Driven Approach for Security Testing, 2007. SESS '07: ICSE Workshops 2007. Third International Workshop on Software Engineering for Secure Systems, 20-26 May 2007, IEEE 2007.

otrzymano / received: 17.01.2013
przyjęto do druku / accepted: 02.12.2013 *artykuł recenzowany / revised paper*

INFORMACJE