Krzysztof Modelewski
OpenSky Systems and Services Sp. z o.o

KONIECZNOŚĆ I OBOWIĄZEK WDROŻENIA POLITYKI BEZPIECZEŃSTWA INFORMACJI W SYSTEMACH ITS

Streszczenie: Artykuł informuje o Systemach Zarządzania Bezpieczeństwem Informacji, mających zastosowanie w Inteligentnych Systemach Transportowych. Praca porusza temat prawnych wymagań dotyczących wdrożenia SZBI i konsekwencji z tym związanych. W tekście opisano normy z serii ISO/IEC 27000, dotyczące wdrażania SZBI w systemach ITS, które zostały oparte na podejściu procesowym PDCA. Istotnymi poruszonymi kwestiami są także analiza ryzyka i audytowanie systemów ITS, które może przynieść zamawiającym znaczne korzyści.
Słowa kluczowe: Inteligentne Systemy Transportowe, ITS, telematyka transportu, systemy zarządzania bezpieczeństwem informacji, SZBI, polityka bezpieczeństwa informacji, PBI, zarządzanie ryzykiem, audytowanie

1. WSTĘP

Wdrożenia Inteligentnych Systemów Transportowych w naszym kraju są coraz bardziej widoczne. Warszawa, Poznań i Olsztyn to tylko niektóre, już istniejące, przykłady „nowoczesnego" podejścia do rozwiązania problemów związanych z zatłoczeniem miast. Termin Inteligentne Systemy Transportowe oznacza szeroki zbiór różnorodnych technologii (telekomunikacyjnych, informatycznych, automatycznych i pomiarowych) oraz technik zarządzania stosowanych w transporcie w celu ochrony życia uczestników ruchu, zwiększenia efektywności systemu transportowego oraz ochrony zasobów środowiska naturalnego [1].

2. ZAGROŻENIA DLA SYSTEMÓW ITS

Kluczowym elementem systemów ITS jest informacja przesyłana za pomocą różnego typu środków łączności. Zastosowanie urządzeń telekomunikacyjnych i informatycznych

sprawia, że systemy ITS są w rzeczywistości systemami teleinformatycznymi (najczęściej opartymi o protokół IP), które podatne są na te same zagrożenia [2]:

a) przerwanie – jest atakiem prowadzącym do zerwania połączenia użytkownika z usługą ITS (np. *call centre*, witryna internetowa przedstawiającą stan warunków na drodze). Może to być np. przypadkowe lub celowe uszkodzenie fizyczne określonego elementu sieci (np. serwera, przewodu).
b) przechwycenie – ma miejsce, gdy osoba niepowołana uzyskuje dostęp do zasobów sieci (np. podsłuch). Ten typ zagrożenia jest niebezpieczny jedynie poprzez fakt, iż atakujący uzyskuje dostęp do poufnych danych, jednak w porównaniu z innymi typami zagrożeń nie ingeruje w ich treść lub samo przesyłanie danych,
c) modyfikacja – polega na zmodyfikowaniu danych przesyłanych przez użytkownika do systemu poprzez zmianę plików, wprowadzenie innych, nieprawdziwych danych.
d) podrobienie – jest atakiem, który polega na podrobieniu przesyłanych danych. W tym przypadku intruz wprowadza nieprawdziwe dane. Modyfikacja i podrobienie są najbardziej niebezpiecznymi typami ataków ze względu na to, iż jeden intruz może wywołać dziesiątki, setki lub tysiące nieprawdziwych powiadomień o wypadkach, paraliżując pracę operatorów w CZR, podawać fałszywe dane dotyczące kursowania pojazdów komunikacji publicznej a także wskazywać błędne informacje na znakach zmiennej treści.

3. WYTYCZNE DOTYCZĄCE SZBI W SYSTEMACH ITS

Przedstawione powyżej zagrożenia mogą być istotnym czynnikiem wpływającym na bezpieczeństwo funkcjonowania systemu transportowego. Stopień wrażliwości na przekłamanie/brak informacji dla poszczególnych kategorii systemów ITS [3] można przyporządkować do klas systemów alarmowych [4].

Tabela 1.

Przyporządkowanie kategorii systemów ITS do klas systemów alarmowych

Kategoria systemu ITS wg ISO TC 204	Klasa systemów alarmowych
Informacja dla podróżnych	SA3
Zarządzanie ruchem	SA3
Pojazd	SA3
Pojazd komercyjny	SA3
Transport publiczny	SA3
Potrzeba pomocy	SA3
Elektroniczne płatności	SA3/SA4
Bezpieczeństwo	SA3

Z powyższej tabeli wynika, iż zabezpieczenia systemów ITS powinny odpowiadać klasie SA3, charakteryzującej się zastosowaniem środków przeciwsabotażowych, która stosowana jest w obiektach o dużym ryzyku szkód. Klasa SA4 może znaleźć zastosowanie

w systemach elektronicznego poboru opłat, gdzie przetwarzane są transakcje o wartości setek tysięcy złotych dziennie i straty wynikające z braku działania systemu byłyby bardzo wysokie. Istotnym aspektem jest także poufność przechowywanych danych osobowych i lokalizacyjnych, uzyskiwanych dzięki systemom nawigacji satelitarnych i technologii DSRC, współpracujących często z system detekcji wizyjnej.

Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (...) realizujących zadania publiczne, w §3 stwierdza, że „Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych. Przy opracowywaniu polityki bezpieczeństwa (...) podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji".

Normy dotyczące Systemów Zarządzania Bezpieczeństwem Informacji (ang. *Information Security Management Systems*) opisują, w jaki sposób należy zaprojektować i utrzymywać system w pełnej sprawności, aby stale odpowiadał zmiennym warunkom otoczenia.

Najnowszą rodziną norm dotyczących SZBI są normy 27000. Spośród wszystkich norm serii 27000, największe znaczenie mają normy ISO 27001 i 27002. Normy te zapewniają kompleksowe podejście do bezpieczeństwa informacji. Ich zapisy dotyczą zarówno informacji papierowej, informacji elektronicznej, jak i wiedzy pracowników [5]. Norma ISO/IEC 27000:2009 *„Information Security Management Systems – Overview and vocabulary"* stanowi wprowadzenie do pozostałych norm. Zawiera słownictwo i terminologię.

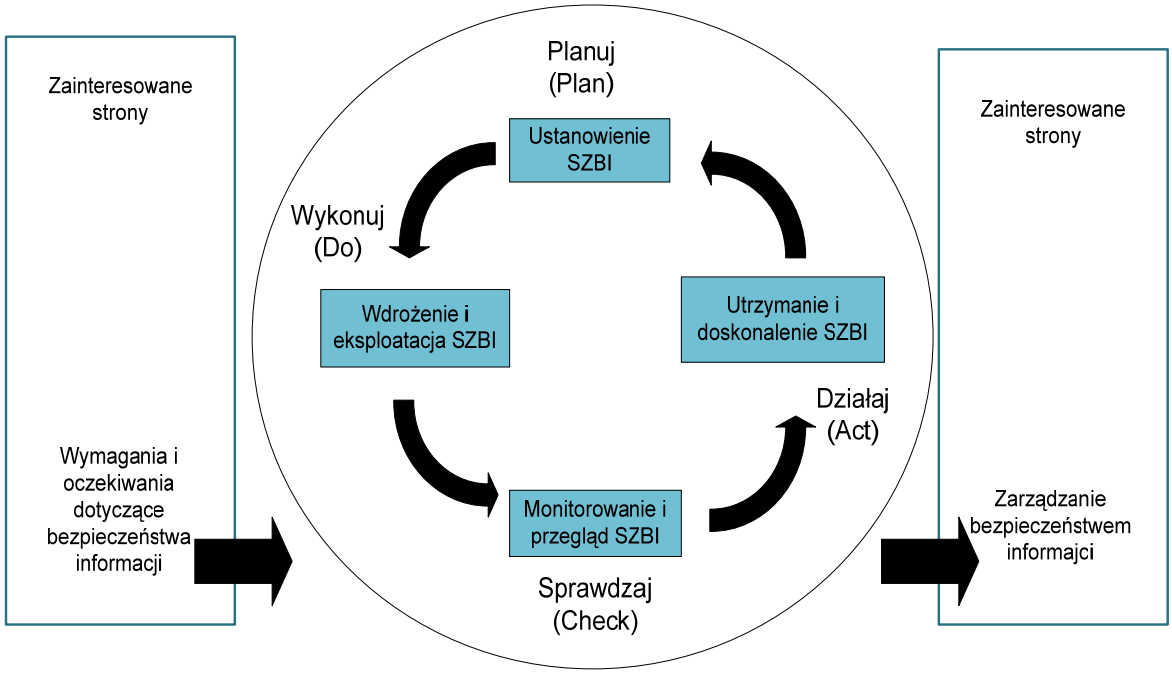
Norma PN-ISO 27001, wprowadzająca ISO/IEC 27001:2005 „Technika informatyczna-Techniki bezpieczeństwa-Systemy zarządzania bezpieczeństwem informacji-Wymagania" jest normą obligatoryjną. „W niniejszej normie zastosowano podejście procesowe w celu ustanawiania, wdrożenia, eksploatacji, przeglądu i doskonalenia SZBI w organizacji"[1] SZBI powinien być zgodny z istniejącym prawem, a udokumentowany za pomocą Polityki Bezpieczeństwa Informacji, w której organizacja określa, w jaki sposób chroni swoje aktywa i realizuje zasady przechowywania i dostępu do informacji. Wszystkie działania dotyczące PBI powinny być zatwierdzone przez kierownictwo, a wszyscy pracownicy powinni być odpowiednio przeszkoleni w zakresie stosowania właściwych procedur. Dodatkowo PBI musi być tak napisana, aby była rozumiana przez wszystkich czytelników, do których jest adresowana. Ma to szczególne znaczenie w kluczowych miejscach, jakimi są Centra Zarządzania Ruchem, w których znajdują się operatorzy oraz urządzenia, służące do przetwarzania i przechowywania danych. Ważnym składnikiem systemów ITS są także urządzenia przydrożne, które powinny być również odpowiednio chronione (bezpieczeństwo sprzętu w CZR i poza nimi, odpowiednia i planowana konserwacja urządzeń i okablowania). Ze względu na to, iż informacja jest jednym z najważniejszych zasobów, należy zapewnić jej ochronę na pożądanym poziomie, tzn. zastosowanie takiego poziomu organizacyjnego i technicznego, który:

– zagwarantuje zachowanie poufności informacji chronionych;
– zapewni integralność informacji chronionych i jawnych oraz dostępność do nich;
– zagwarantuje wymagany poziom bezpieczeństwa przetwarzanych informacji;

[1] PN-ISO/IEC 27001

– maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji;
– zapewni poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji;
– zapewni gotowość do podejmowania działań w sytuacjach kryzysowych. [6]

Opisane w normie podejście procesowe polega na tym, że wyjście z danego procesu wpływa na wejście kolejnego. Zdefiniowano cztery stany zarządzania bezpieczeństwem, które zostały przedstawione na rys. 1.



Rys. 1. Model PDCA (ang. *Plan, Do, Check, Act*)

Planowanie SZBI – podjęcie decyzji o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji jest decyzją strategiczną. Organizacja zarządzająca danym systemem ITS powinna m.in. zdefiniować zakres i granice SZBI, określić ryzyka oraz zdefiniować politykę SZBI.

Wdrożenie i eksploatacja SZBI – na tym etapie należy wdrożyć odpowiednie zabezpieczenia, opracować procedury postępowania w przypadku zaistnienia danego ryzyka, np. awarii kluczowych elementów sieci teleinformatycznej. Istotnym zagrożeniem są stosowane przez napastników socjotechniki, czyli metody używane w celu wzbudzenia zaufania [7, 8]. Ważnym zadaniem przeciwdziałania tym atakom jest uświadamianie pracowników poprzez np. system szkoleń definiujących, jakie informacje należy uważać za poufne i jak z nimi postępować.

Monitorowanie i przegląd SZBI – SZBI jest systemem opartym o ciągłe doskonalenie. Na tym etapie organizacja zarządzająca powinna okresowo wykonywać procedury monitorowania i przeglądu, badać skuteczność zabezpieczeń oraz uaktualniać plany bezpieczeństwa.

Utrzymanie i doskonalenie SZBI – organizacja powinna w sposób ciągły doskonalić i podejmować odpowiednie procedury korygujące i zapobiegawcze, eliminujące wcześniej powstałe błędy.

Tabela 2.

Model PDCA (źródło: ISO 27000)

Proces	Opis procesu
Planuj (ustanowienie SZBI)	Ustanowienie polityki SZBI, celów, procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji, tak, aby uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji
Wykonaj (wdrożenie i eksploatacja SZBI)	Wdrożenie i eksploatacja polityki SZBI, zabezpieczeń, procesów
Sprawdzaj (monitorowanie i przegląd SZBI)	Szacowanie i tam gdzie ma zastosowanie, pomiar wydajności procesów w odniesieniu do polityki SZBI, celów i doświadczenia praktycznego oraz dostarczanie kierownictwu raportów do przeglądu
Działaj (utrzymanie i doskonalenie SZBI)	Podejmowanie działań korygujących i zapobiegawczych w oparciu o wyniki wewnętrznego audytu SZBI i przeglądu realizowanego przez kierownictwo lub innych istotnych informacji, w celu zapewnienia ciągłego doskonalenia SZBI

Istotnym elementem w opracowywaniu Polityki Bezpieczeństwa Informacji jest szacowanie ryzyka. Opisywane jest ono przez wiele metodyk, m.in. zawartych w raporcie technicznym ISO/IEC 13335-3 „Information Technology – Guidelines for the management of IT Security – Techniques for the management of IT Security" Szacowanie ryzyka to całościowy proces analizy i oceny ryzyka. Należy zdefiniować zdarzenia, które mogą spowodować zakłócenie pracy systemu wraz z określeniem prawdopodobieństwa wystąpienia oraz jego konsekwencjami. W PBI powinno się także opracować i wdrożyć plany utrzymania lub odtworzenia systemu po wystąpieniu przerwy lub awarii krytycznych zasobów. Ryzyko może być minimalizowane także za pomocą przenoszenia go na inne podmioty.

Rodzina norm ISO/IEC 27000 zawiera także normy ogólne:

a) ISO/IEC 27002 (polski odpowiednik to norma PN-ISO/IEC 17799:2007) – opisuje praktyczne zasady zarządzania bezpieczeństwem informacji.
b) Norma ISO/IEC 27003 – to przewodnik implementacji SZBI.
c) Norma ISO/IEC 27004 – opisuje pomiary dotyczące SZBI.
d) Norma ISO/IEC 27005 – to przewodnik do aspektów zarządzania ryzykiem.
e) Norma ISO/IEC 27006 – zawiera wytyczne dla jednostek prowadzących audyty i certyfikacje Systemów Zarządzania Bezpieczeństwem Informacji, jako uzupełnienie wymagań zawartych w ISO/IEC 17021 i ISO/IEC 27001. Norma obligatoryjna.
f) Norma ISO/IEC 27007 – zawiera wytyczne do zarządzania systemem audytów SZBI.

Wydany przez IETF[2] w 1997 roku dokument RFC 2196 [9] „Site Security Handbook" jest praktycznym dokumentem, opisującym zagrożenia związane zarówno z technicznymi

[2] Internet Engineering Task Force

aspektami bezpieczeństwa informatycznego (m.in. zabezpieczenie usług sieciowych, i protokołów routingu), jak i aspektami nietechnicznymi (reagowanie i postępowanie w przypadku wystąpienia incydentów, dostęp fizyczny itd.). Stanowi on pomoc dla administratorów sieci,

4. AUDYTOWANIE SYSTEMÓW ITS

Zadaniem audytu jest rzetelna ocena organizacji, systemu, procesu, osoby, projektu lub produktu, przeprowadzona na podstawie określonych danych, wymagań i standardów. Audyt może być szczególnie przydatny w celu weryfikacji jakości zamówionego systemu ITS. Często instytucja zlecająca nie ma odpowiednich zasobów, aby móc zweryfikować jakość elementów systemu, np. zgodność architektury z ustaleniami kontraktowymi [10]. W takim przypadku możliwe jest zlecenie audytu obiektywnej jednostce zewnętrznej. Audyt wewnętrzny jest możliwy jedynie wtedy, gdy organizacja ma wykwalifikowanych pracowników, potrzebnych aby stworzyć zespół audytujący. Często ten rodzaj audytu trwa dłużej, gdyż jednostka zewnętrzna, wyspecjalizowana w tym zakresie, ma doświadczenie i metodyki, pozwalające na znaczne skrócenie czasu jego trwania. Normami i zbiorami dobrych praktyk, według, których można przeprowadzać audyt, są normy serii ISO 9001, część norm z serii ISO/IEC 27000, metodyki ITIL (ang. *Information Technology Infrastructure Library*) i COBIT *(Control Objectives for Information and related Technology*).

5. PODSUMOWANIE

Bezpieczeństwo systemów ITS jest kluczowe dla zapewnienia ciągłości działania usług ITS. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji powinna być w określonych odstępach czasu przeglądana i weryfikowana, aby dokument PBI był cały czas aktualny, a cele pozostały jasne i czytelne. W systemach ITS należy położyć duży nacisk na kształcenie kadry kierowniczej, operatorów i techników pod względem bezpieczeństwa systemu, a także dostępu do informacji, pomieszczeń i urządzeń znajdujących się w terenie.

W analizie ryzyk oraz ocenie jakości systemów ITS pomocne są audyty, wykonywane przez niezależnych ekspertów. Szczegółowa analiza oparta o standardy i znane na całym świecie metodyki pozwoli na bezpieczne i ciągłe działanie usług ITS, które służą coraz większej liczbie osób.

Bibliografia:

1. Modelewski, K. „Czym jest ITS?”, strona internetowa Stowarzyszenia „ITS Polska”, www.itspolska.pl, 20 marzec 2010 r.

2. Rychlicki M. „Zastosowania Systemu Elektronicznego powiadamiania o wypadkach", VIII Międzynarodowa Konferencja TST, Ustroń 2006
3. ISO TC 204, http://www.iso.org
4. Klasy systemów alarmowych, Polska Norma Systemy alarmowe PN-93/E-08390 z 1 stycznia 1994 r.
5. Guzik, A. „SZBI receptą na bezpieczeństwo informacji", Haking, nr 3/2010
6. Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego, kwartalnik Telekomunikacja i Techniki Informacyjne (TiTI), 3-4/2007
7. Mitnick, K., „Sztuka Podstępu, Łamałem ludzi, nie hasła", Wyd. Helion, 2003
8. Mitnick, K., Simon W.L. „Sztuka Infiltracji, czyli jak włamywać się do sieci komputerowych", Wyd. Helion, 2006
9. IETF, „RFC 2196, Site Security Handbook", http://datatracker.ietf.org, 30 marzec 2010 r.
10. Zimtrowicz K. „Audyt techniczny. Czyli jak sprawdzić jakość pracy dostawcy IT?, Software Developer's Journal, nr 3/2010

NECESSITY AND OBLIGATION FOR INFORMATION SECURITY MANAGEMENT SYSTEMS IMPLEMENTATION IN INTELLIGENT TRANSPORT SYSTEMS

Abstract: The paper informs about the Information Security Management Systems, as applied to Intelligent Transport Systems. It brings up the subject of legal requirements concerning ISMS implementation, and associated consequences. The author describes the ISO/IEC 27000 standards, based on the PDCA (Deming) cycle. Important topics are also risk management and ITS auditing, which may bring substantial benefits to the buyers.
Keywords: Intelligent Transport Systems, Information Security Management Systems, auditing