STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Andrzej BIAŁAS
Wyższa Szkoła Informatyki i Zarządzania w Bielsku-Białej

WYSOKOPOZIOMOWE MODELOWANIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Streszczenie. W artykule zaproponowano zapis formalny referencyjnego modelu bezpieczeństwa oraz przedstawiono proces jego kompilacji w system bezpieczeństwa instytucji. Na podstawie stopnia uzależnienia funkcjonowania instytucji od zaangażowania w to środków teleinformatycznych wyznaczane są cele, strategie i polityki bezpieczeństwa na poziomie instytucji, wyrażające jej ogólne potrzeby w tym zakresie. Na tej podstawie wypracowywane są wymagania dotyczące bezpieczeństwa teleinformatycznego w instytucji, a te z kolei przekładają się na szczegółowe zasady bezpieczeństwa każdego z eksploatowanych w niej systemów. Artykuł przedstawia ogólny schemat postępowania przy tworzeniu systemu bezpieczeństwa instytucji, który stwarza szanse na automatyzację tych działań.

Słowa kluczowe: bezpieczeństwo teleinformatyczne, wysokopoziomowa analiza ryzyka, modelowanie własności bezpieczeństwa, zarządzanie.

HIGH LEVEL ICT SECURITY MODELLING

Summary. The paper presents the high-level security model compatible with common IT security objectives, strategies and policies concept. It expresses business level security needs. This is the base for defining the security objectives, strategies and policies for the considered organisation. Analysing strategies in the context of objectives and policies, general ICT security level is defined. Next, on this base, security for any ICT system can be precisely expressed. The paper presents general compilation scheme of this model.

Keywords: ICT security management, high-level risk analysis, ICT security modelling.

1. Wprowadzenie

Artykuł przedstawia koncepcję budowy modelu bezpieczeństwa teleinformatycznego instytucji na wysokim poziomie ogólności (*ang. high level security model*). We właściwy sposób pozwala on ująć relacje, w tym kosztowe, między potrzebami bezpieczeństwa wynikającymi z zaangażowania technologii teleinformatycznych do realizacji zadań statutowych (misji) instytucji, a docelowo zastosowanymi zabezpieczeniami. Potrzeby bezpieczeństwa instytucji wynikają z powagi zadań biznesowych i stopnia zaangażowania teleinformatyki w ich realizację. Te potrzeby należy przetransponować na szczegółowe wymagania, jakie muszą spełniać systemy, a te z kolei na szczegółowe zasady i środki dotyczące zabezpieczeń. Właściwe ujęcie tego typu związków pozwala na dobór zabezpieczeń adekwatnych do wartości chronionych zasobów. Analiza tych zależności stanowi element tak zwanej **wysokopoziomowej analizy ryzyka** w systemach teleinformatycznych (*ang. High level risk analysis*).

Zaproponowany wysokopoziomowy model bezpieczeństwa jest zgodny z trójpoziomowym modelem celów, strategii polityk [1], [2], [5], który stanowi model referencyjny do budowy wszelkich systemów bezpieczeństwa. Niżej prezentowany model jest jedną z możliwych prób formalnego zapisu zawartych tam koncepcji. Ze względu na obszerność tych zagadnień w artykule ograniczono się do przedstawienia ogólnej koncepcji modelu, popartej przykładem z dziedziny gospodarki elektronicznej.

2. Zapis formalny wysokopoziomowego modelu bezpieczeństwa

Bezpieczeństwo rozpatrywane jest na trzech poziomach (rys. 1):

- Poziom I – instytucja wykorzystująca technologie teleinformatyczne do realizacji swych zadań statutowych – zapewnienie ciągłości jej funkcjonowania (procesów biznesowych, misji) w sytuacji zagrożeń i zmian w otoczeniu;
- Poziom II – ogół systemów teleinformatycznych instytucji; w przypadku rozbudowanych wielooddziałowych instytucji wyróżnia się opcjonalnie dodatkowy podpoziom oddziału – oznaczmy go IIa;
- Poziom III – poszczególne systemy eksploatowane w instytucji.

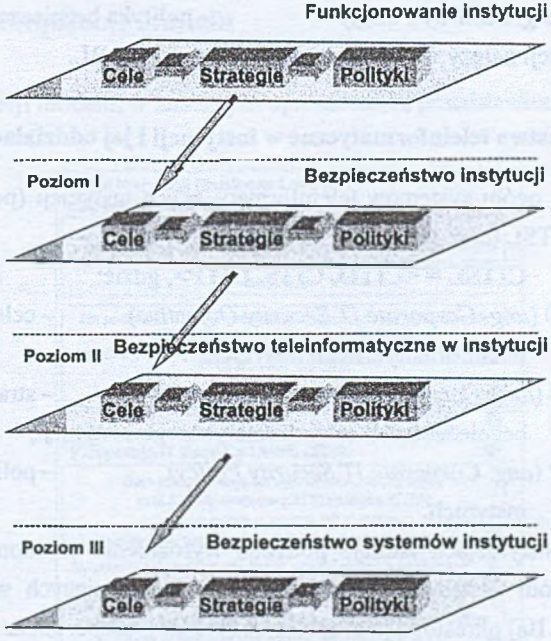
Dla każdego szczebla organizacji lub obszaru działania instytucji można zdefiniować:

- **cel** – identyfikuje to, co ma być osiągnięte,
- **strategię** – która przedstawia, jak osiągnąć wytyczony cel,
- **polityki** – podaje, co musi być konkretnie wykonane.

Występują dwa rodzaje zależności:

- **poziome** - z celów wynikają strategie, a te są rozpracowywane do polityk,
- **pionowe** - trójka cel, strategia, polityka niższego poziomu stanowi konkretyzację (uszczegółowienie) sformułowań z wyższego poziomu; należy zwrócić uwagę na charakterystyczne przełożenie strategii wyższego poziomu na cel poziomu niższego.

Powyższe założenia ogólne legły u podstaw zastosowanej w modelu notacji formalnej, która z kolei umożliwia przedstawienie procesu stopniowego uszczegółowienia modelu w system bezpieczeństwa. Ze względu na obszerność zagadnień proces ten mógł być jedynie naszkicowany w niniejszym artykule. Z natury jest on bardzo złożony i wieloetapowy, przy tym występują w nim liczne sprzężenia zwrotne. Dalej będzie on określany jako **proces kompilacji modelu**.



Rys. 1. Cele, strategie i polityki w modelu trójpoziomowym
Fig. 1. Objectives, strategies and policies within hierarchical security model

2.1. Bezpieczeństwo w instytucji

Zadania statutowe instytucji (misja) – komercyjne, administracyjne, militarne lub inne określa się za pomocą czwórki BL (*ang. Business Level*):

BL = <BO, BS, BP, DD>, gdzie:

BO (*ang. Business Objective*) – cele działania, czyli zadanie statutowe;

BS (*ang. Business Strategy)* – strategie osiągnięcia celu działania;

BP (*ang. Business Policy)* – polityka działania instytucji;

DD (*ang. Dependency Degree)* – umowny poziom zaangażowania środków teleinformatycznych w realizację danego celu działania instytucji – wyraża uzależnienie realizacji celów od pracy systemów teleinformatycznych i towarzyszące temu ryzyko biznesowe.

Bezpieczeństwo funkcjonowania instytucji (poziom I) określa się za pomocą trójki BLS (*ang. Business Level Security*):

BLS = <SO, SS, SP>, gdzie:

SO (*ang. Security Objective*) – cele bezpieczeństwa instytucji;

SS (*ang. Security Strategy)* – strategie bezpieczeństwa instytucji;

SP (*ang. Security Policy)* – polityka bezpieczeństwa instytucji.

Na poziomie instytucji należy wyrazić związki między BLS a BL.

2.2. Bezpieczeństwo teleinformatyczne w instytucji i jej oddziałach

Bezpieczeństwo ogółu systemów teleinformatycznych instytucji (poziom II) określa się za pomocą trójki CITSL (*ang. Corporate IT Security Level*):

CITSL = <CITO, CITS, CITP>, gdzie:

CITO (*ang. Corporate IT Security Objective*) – cele bezpieczeństwa teleinformatycznego instytucji;

CITS (*ang. Corporate IT Security Strategy)* – strategie bezpieczeństwa teleinformatycznego instytucji;

CITP (*ang. Corporate IT Security Policy)* – polityka bezpieczeństwa instytucji.

W niektórych instytucjach istnieje potrzeba wyróżnienia autonomicznych oddziałów. Bezpieczeństwo ogółu systemów teleinformatycznych działających w oddziale instytucji (opcjonalny poziom IIa) określono jako trójka DITSL (*ang. Department IT Security Level*):

DITSL = <DITO, DITS, DITP>, gdzie:

DITO (*ang. Department IT Security Objective*) – cele bezpieczeństwa teleinformatycznego oddziału instytucji;

DITS (*ang. Department IT Security Strategy)* – strategie bezpieczeństwa teleinformatycznego oddziału instytucji;

DITP (*ang. Department IT Security Policy)* – polityka bezpieczeństwa teleinformatycznego oddziału instytucji.

2.3. Bezpieczeństwo poszczególnych systemów teleinformatycznych eksploatowanych w instytucji

Bezpieczeństwo konkretnego sytemu teleinformatycznego działającego w instytucji lub jej oddziale (poziom III) przedstawia trójka ITSSL (*ang. IT System Security Level*):

ITSSL = <ITSO, ITSS, ITSP>, gdzie:

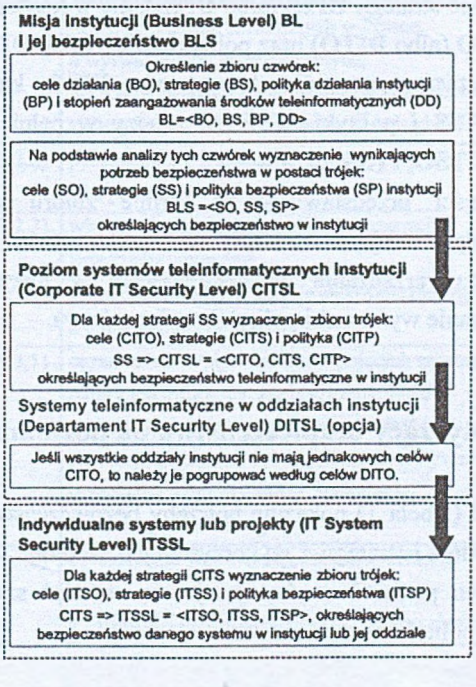
ITSO (*ang. IT System Security Objective*) – cel bezpieczeństwa danego systemu;

ITSS (*ang. IT System Security Strategy)* – strategia bezpieczeństwa systemu;

ITSP (*ang. IT System Security Policy)* – polityka bezpieczeństwa systemu.

3. Przebieg kompilacji modelu

Przebieg kompilacji modelu, w znacznym uproszczeniu, przedstawiono na rys. 2.



Rys. 2. Ogólny schemat kompilacji modelu
Fig. 2. General compilation scheme

Przebieg kompilacji (uszczegółowiania) modelu można wyrazić następująco:

1. Na podstawie analizy zadań statutowych (procesów biznesowych) realizowanych przez instytucję identyfikowane są trójki **<BO, BS, BP>**.
2. Dla każdej trójki przedstawia się **DD**, czyli stopień zaangażowania środków teleinformatycznych w realizację celu biznesowego i związane z tym **ryzyko** – w ten sposób w pełni zdefiniowany zostaje poziom **BL = <BO, BS, BP, DD>**.
3. Zaangażowanie środków teleinformatycznych i związane z tym ryzyko rodzi określone potrzeby dotyczące bezpieczeństwa, które można wyrazić, formułując cele bezpieczeństwa instytucji **SO**, z których wynikają strategie **SS** oraz polityki **SP**, co pozwala zdefiniować bezpieczeństwo w instytucji jako: **BLS = <SO, SS, SP>**.
4. Strategie **SS**, ale w kontekście **SO** i **SP**, przekładane są na cele bezpieczeństwa **CITO**, dla których należy wskazać strategie realizacji **CITS** i wypracować politykę **CITP**, to znaczy w pełni zdefiniować poziom II: **CITSL = <CITO, CITS, CITP>**.
5. W instytucjach posiadających oddziały różniące się pod względem celów **CITO** należy podzielić je na grupy **DITO**, odpowiadające specyfice oddziałów.
6. Na podstawie strategii **CITS** (albo **DITS**), ale w kontekście odpowiadających im celów **CITO** (albo **DITO**) oraz polityki **CITP** (albo **DITP**), formułowane są cele bezpieczeństwa poszczególnych systemów **ITSO**, które należy przełożyć na strategie **ITSS** i polityki **ITSP**, to znaczy w pełni zdefiniować poziom III: **ITSSL = <ITSO, ITSS, ITSP>**.

Powyższe zależności przedstawiono w formie zbioru szablonów, dla których opracowywane są odpowiadające struktury w języku XML, co umożliwia budowę szkieletowego systemu zarządzania bezpieczeństwem w instytucji, pozwalającego na automatyczne generowanie wymagań i polityk bezpieczeństwa.

4. Przykład dotyczący bezpieczeństwa na poziomie instytucji

Niniejszy przykład (tabela 1) pokazuje potrzeby bezpieczeństwa księgarni internetowej wyrażone w postaci celów i strategii z wykorzystaniem szablonu BLS_tpl, stosowanego dla poziomu BLS. Na tym poziomie wykorzystuje się również szablon SP_tpl służący do wyrażenia dokumentu polityki bezpieczeństwa.

Tabela 1

Bezpieczeństwo na poziomie instytucji

SO Cele bezpieczeństwa instytucji		**SS** Strategie bezpieczeństwa instytucji - *„poprzez"*		**SP** Polityka bezpieczeństwa instytucji
SO(i)	Opis słowny	SS(i,j)	Opis słowny	SP - komentarz
SO(1)	Zapewnić ciągłość realizacji zadań statutowych	SS(1,1)	ograniczenie wpływu szeroko pojętych zagrożeń natury teleinformatycznej (systemy, ludzie, organizacja) do poziomu akceptowalnego i kontrolowanego	Po przeanalizowaniu informacji znajdujących się w kolumnach położonych na lewo i zastosowaniu szablonu SP_tpl, sformułowane są wnioski i inne towarzyszące im postanowienia, które zostaną zawarte w tak zwanym dokumencie polityki bezpieczeństwa instytucji.
		SS(1,2)	zapewnienie wysokiego poziomu niezawodności i dostępności usług oferowanych przez systemy, z możliwością tolerowania jedynie krótkotrwałych upadków	
		SS(1,3)	utrzymywanie wysokiego, adekwatnego do potrzeb instytucji poziomu poufności, integralności, dostępności i jakości informacji, niezależnie od jej postaci	
SO(2)	Zapewnić działania zgodne z prawem	SS(2,1)	właściwą ochronę informacji zaliczanych do tajemnic prawnie chronionych w Polsce, a wytwarzanych, przetwarzanych, przechowywanych i przekazywanych za pomocą systemów, zwłaszcza tajemnicy przedsiębiorstwa	
		SS(2,2)	poszanowanie istniejących aktów prawnych, w tym prawa autorskiego	
		SS(2,3)	właściwą ochronę informacji, związanych z zawartymi umowami	
		SS(2,4)	świadczenie usług w formie elektronicznej zgodnie z obowiązującym prawem	
SO(3)	Zapewnić ochronę wizerunku i reputacji firmy	SS(3,1)	ograniczenie wpływu szeroko pojętych zagrożeń natury teleinformatycznej (systemy, ludzie, organizacja), które mogłyby zaszkodzić jej reputacji, zwłaszcza cybergraffiti, wywoływanie przeciążeń, odmowy usług, ujawnienie chronionych informacji itp.	
		SS(3,2)	ograniczenie wpływu zagrożeń dla realizacji zobowiązań zewnętrznych, wynikających z zawartych umów oraz z zasad dobrego obyczaju	

5. Wnioski i uwagi końcowe

Artykuł przedstawia jedynie szkic wysokopoziomowego modelu bezpieczeństwa zgodnego z modelem referencyjnym [2]. Model wysokopoziomowy pozwala wyrazić własności bezpieczeństwa od ogółu (potrzeby misji instytucji) po szczegóły polityki zabezpieczeń. Może być implementowany w postaci szablonów lub struktur zapisanych w języku XML, co z kolei umożliwia tworzenie programowych narzędzi wspomagających.

Optymalizacja tych struktur, zwłaszcza pod kątem poprawy spójności, wymuszania precyzji sformułowań podczas warsztatów wysokopoziomowej analizy ryzyka, wyrażania skomplikowanych zależności występujących w systemie bezpieczeństwa, stanowi wyzwanie do prowadzenia dalszych prac w tym obszarze.

LITERATURA

1. ISO/IEC TR 13335-1: 1996, Information technology – Guidelines for the management of IT Security, Part1: Concepts and models for IT Security.
2. PN-I-13335-1: Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. PKN, styczeń 1999.
3. Białas A.: Zarządzanie bezpieczeństwem informacji w systemach gospodarki elektronicznej. VIII Konferencja SIECI KOMPUTEROWE – Krynica 2001. Studia Informatica vol. 22, Number 2(44), Silesian University of Technology, Gliwice 2001.
4. Białas A.: Wprowadzenie do modelowania procesów analizy ryzyka w systemach teleinformatycznych. IX Konferencja SIECI KOMPUTEROWE – Zakopane 2002. Studia Informatica vol. 23, Number 2B(49), Silesian University of Technology, Gliwice 2002.
5. Białas A. (red. pracy zbiorowej): Bezpieczeństwo systemów teleinformatycznych – Podręcznik do szkoleń autoryzowanych przez Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002.
6. Project SPARTA: Security Policy Adaptation Reinforced Through Agents - http://www.infosys.tuwien.ac.at/sparta
7. Sipponen M.T.: Policies for Construction of Information Systems' Security Guidelines, Proceedings of 16th IFIP TC11 Annual Working Conference, Beijing, August 2000.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 24 marca 2003 r.

Abstract

The paper deals with ICT security modelling on the high level. The presented model is compatible with common IT security objectives, strategies and policies concept. Model is able to express security features, starting on the highest (organizational) level, through ICT security, to any system security level (Fig 1). On the Fig. 2, the general compilation scheme is presented, showing how more and more detailed description is achieved. Model notation can be based on the templates or XML structures, allowing software implementation. An example of fulfilled template for the Internet bookstore is shown in the table 1.

Adres

Andrzej BIAŁAS: Wyższa Szkoła Informatyki i Zarządzania, ul. Legionów 81,
43-300 Bielsko-Biała, Polska, abialas@wsi.edu.pl .