Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/EPU.2018.131/1-34 | strony: 347–360

Jerzy Stanik, Maciej Kiedrowicz
Wojskowa Akademia Techniczna
Wydział Cybernetyki
jerzy.stanik@wat.edu.pl, maciej.kiedrowicz@wat.edu.pl

Raport analizy ryzyka jako kluczowy element tworzenia polityki bezpieczeństwa informacji

Kody JEL: D81, D82, D83
Słowa kluczowe: bezpieczeństwo informacji, polityka bezpieczeństwa, analiza ryzyka
Streszczenie. Autorzy przedstawiają autorskie podejście do procesu tworzenia i utrzymywania polityki bezpieczeństwa informacji w organizacji. Zaproponowany sposób tworzenia polityki bezpieczeństwa ma charakter kompleksowy i łatwy do zastosowania w praktyce. Opiera się na takim cyklu życia polityki bezpieczeństwa, którego etapem startowym są prace przygotowawcze wykonywane dość rzadko i na żądanie, zaś etapem zasadniczym są prace wykonywane cyklicznie – model PDCA[1]. W ramach każdego cyklu wykonywane są następujące procesy: przeprowadzenie analizy ryzyka, opracowanie projektu Bazowej Polityki Bezpieczeństwa Informacji (BPBI), wdrożenie projektu, opracowanie strategii zabezpieczeń, ocena skuteczności zrealizowanej strategii, doskonalenie polityki bezpieczeństwa.

Wprowadzenie

W procesie tworzenia, rozwoju i doskonalenia polityki bezpieczeństwa (PB) bardzo istotnym elementem jest sam moment rozpoczęcia tego procesu. Istnieje wiele publikacji, opracowań oraz dokumentów standaryzujących (PN-ISO/IEC 27001 [2014];

[1] PDCA – schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia, Kaizen), stworzoną przez Williama Edwardsa Deminga.

ISO/IEC 27002 [2014]; RFC 2196 [1997]; FIPS PUB 191 [1994]) opisujących różne modele cyklu życia Dokumentu Polityki Bezpieczeństwa (DPB)[2].

W pracach o charakterze norm lub dokumentów standaryzujących (ISO/IEC 27002 [2014]; http://eur-lex.europa.eu [2018]) sugeruje się rozpoczynanie tego procesu od opracowania kompleksowego programu opracowania i wdrożenia Polityki Bezpieczeństwa Informacji, który za każdym razem należy dostosować do bieżących potrzeb organizacji klienta.

W pracach o charakterze komercyjnym sugeruje się samodzielne sporządzanie, „od zera", korzystając z wiedzy i doświadczeniu fachowców na co dzień trudniących się zagadnieniami bezpieczeństwa informacyjnego.

W pracach o charakterze ogólnodostępnych stron internetowych, np. (http://www.faqs.org [2017]; http://www.itl.nist.gov [2017[) autorzy doradzają lub sugerują rozpoczynanie tego żmudnego procesu od:

- wyboru jednego ze zbioru powszechnie dostępnych wzorców polityk, a następnie prowadzić szereg czynności zorientowanych na przystosowywanie treści tego wzorca do potrzeb organizacji w zakresie bezpieczeństwa,
- od wyznaczenia osoby zarządzającej całokształtem działań związanych z zapisywaniem zbioru reguł i procedur, według których dana organizacja będzie budować, zarządzać oraz udostępniać zasoby i systemy informacyjne.

Powstaje również coraz więcej publikacji specjalistycznych opisujących sposoby lub metody tworzenia Polityki Bezpieczeństwa Informacji (PBI), których autorzy doradzają rozpoczynanie procesu od opracowania Szczególnych Wymagań Bezpieczeństwa, a następnie uzupełniać i rozwijać zbiór tych specyfikacji do postaci mających charakter elementów polityki bezpieczeństwa organizacji.

Przedstawione rozważania (na tle przeglądu norm, standardów i różnych typów publikacji) pozwalają stwierdzić, że rozpoczynanie cyklu życia dokumentu PB od, np.: wyboru jednego ze zbioru powszechnie dostępnych wzorców polityki lub wyznaczenia osoby zarządzającej całokształtem działań związanych z zapisywaniem zbioru reguł i procedur i itp., **nie jest** rozwiązaniem w pełni przydatnym, ponieważ:

- problem dokonania takiego spisu lub naśladowania wzorca nie jest trywialny i zależy od wielu innych zapisów wynikających z funkcjonowania organizacji (np. przeprowadzonych audytów jakości lub bezpieczeństwa, przeprowadzonej analizy ryzyka itp.),
- polityka bezpieczeństwa w miarę upływu czasu musi stale uwzględniać nowe warunki (nowe zagrożenia i podatności zasobów informacyjnych, nowe dokonane zmiany w systemie informacyjnym, np. nowe technologie, rotację pracowników itp.) – w przeciwnym przypadku staje się bezużyteczna.

---

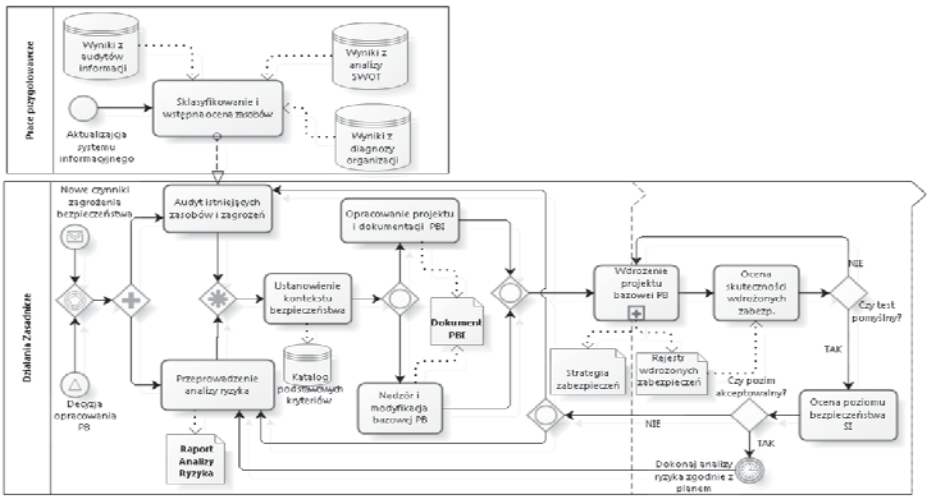
[2] Termin „cykl życia DPB" określa koncepcję rozłożenia w czasie głównych czynności podczas pracy nad opracowaniem i wyprodukowaniem dokumentu Polityki bezpieczeństwa oraz podczas jego eksploatacji i doskonalenia.

Reasumując można stwierdzić, że w większości wymienionych prac lub zalecanych praktyk, proces tworzenia i kontroli dokumentu polityki bezpieczeństwa ma charakter podejścia indywidualnego.

Celem artykułu jest zaproponowanie innego niż powszechnie stosowanego sposobu tworzenia Polityki Bezpieczeństwa Informacji (PBI). Przedstawiony sposób ma charakter podejścia kompleksowego, uwzgledniającego nie tylko działania zasadnicze, ale również prace przygotowawcze, znacznie ułatwiające późniejsze prowadzenie prac zasadniczych. Jest on również łatwy do zastosowania w praktyce.

1. Model cyklu życia Polityki Bezpieczeństwa Informacji

Schematyczną ilustrację tworzenia Polityki Bezpieczeństwa Informacji (PBI) przedstawiono na rysunku 1.



Rysunek 1. Ilustracja tworzenia polityki bezpieczeństwa informacji z punktu widzenia kluczowej roli raportu analizy ryzyka

Źródło: opracowanie własne.

Na rysunku 1 pokazano, że podstawowymi składowymi modelu cyklu życia PBI są dwie fazy obejmujące:

1. Prace przygotowawcze – faza realizowana jednorazowo lub bardzo rzadko.
2. Działania zasadnicze – faza realizowana cyklicznie i dość często.

1.1. Etap prac przygotowawczych

Do zbioru prac przygotowawczych można zaliczyć:

- analizę SWOT,

- audyt wstępny lub wewnętrzny systemu informacyjnego na potrzeby bezpieczeństwa informacji organizacji,
- diagnozę zasobów informacyjnych i zagrożeń,
- identyfikowanie, klasyfikowanie i wartościowanie aktywów organizacji.

Podstawowymi wynikami prac przygotowawczych powinny być:

1. Wyniki z analizy SWOT – w pierwszym kroku analizuje się zewnętrzne aspekty działania organizacji, które mają wpływ na wybór strategii zabezpieczeń (zagrożenia, środki i sposoby zabezpieczeń). W drugim kroku należy dokonać analizy wewnętrznych mocnych (odporność zasobów) i słabych (podatność zasobów) stron organizacji oraz jej kultury pracy. Trzeci krok to wykorzystanie wyników analizy SWOT i opracowanie projektu polityki bezpieczeństwa oraz strategii zabezpieczeń.
2. Wyniki z audytu wewnętrznego Systemu Informacyjnego (ASI) – identyfikacja luk informacyjnych, schemat obiegu informacji w przedsiębiorstwie; wizualizacja (*mapping*) przepływów informacji i barier w jej przepływie, katalog zasobów informacyjnych organizacji i ocena ich wartości dla organizacji; lokalizacje punktów „produkcji" informacji, metody jej tworzenia i przetwarzania, a także kanały przepływu, baza wykorzystania wewnętrznych źródeł informacji, ocena ich wartości; charakterystyki technologii wykorzystywanych do gromadzenia, przetwarzania i rozpowszechniania danych korzyści płynące z usprawnienia obiegu informacji w przedsiębiorstwie (można je podzielić na wewnętrzne i zewnętrzne).
3. Wyniki z diagnozy organizacji – dokument w formie elektronicznej pt. „Diagnoza stanu Organizacji" w postaci analitycznego raportu zawierającego: opis stanu bezpieczeństwa informacji w organizacji, wyniki z przeglądu dokumentacji systemu zarządzania organizacji, a w szczególności z analizy ryzyka związanego z bezpieczeństwem informacji oraz deklaracji stosowania, wyniki z oceny lokalizacji i obiegu zasobów informacyjnych organizacji, zbierane dowody zgodności systemu zarządzania bezpieczeństwem informacji z normą PN-ISO/IEC 27001.
4. Dane ze sklasyfikowania i wstępnej oceny wartości zasobów informacyjnych – katalog zasobów informacyjnych zawierający dane dotyczące wykorzystujących rodzajów zasobów informacyjnych w systemie informacyjnym oraz aplikacji i nośników używanych do ich przetwarzania; dane zebrane w pierwszym kroku są następnie klasyfikowane pod względem ich wartości dla organizacji.

1.2. Faza prac zasadniczych

Zbiór działań zasadniczych można zdekomponować na następujące procesy:

1. Proces zarządzania ryzykiem obejmujący następujące działania:
   - ustalanie podstawowych kryteriów oceny ryzyka w bezpieczeństwie informacji w organizacji. Kryteria brane pod uwagę to m.in.: ogólny stopień

poufności, skutki utraty lub modyfikacji danego zasobu informacyjnego, koszt początkowy, koszt zastąpienia lub odtworzenia, wartość dobrego imienia organizacji itp. Zaleca się, aby kryteria stosowane jako podstawa do przypisywania wartości wszystkim zasobom informacyjnym były opisane za pomocą jednoznacznych określeń. Często jest to jeden z najtrudniejszych aspektów wartościowania zasobów, ponieważ wartości części zasobów mogą być określane subiektywnie i przeważnie takie wartościowanie wykonuje wiele różnych osób,
   - prowadzenie analizy i szacowania ryzyka.
2. Proces tworzenia bazowej polityki bezpieczeństwa obejmujący:
   - opracowanie projektu i bazowej dokumentacji Polityki Bezpieczeństwa,
   - ciągły nadzór, kontrola i modyfikacja istniejącej bazowej Polityki Bezpieczeństwa Informacji.
3. Proces wdrożenia projektu Bazowej Polityki Bezpieczeństwa obejmujący następujące podprocesy:
   - opracowywania strategii zabezpieczeń,
   - implementacji i wdrażania zabezpieczeń,
   - oceny skuteczności wprowadzonych zabezpieczeń.
4. Proces zarządzania ryzykiem obejmujący następujące działania:
   - ocena poziomu bezpieczeństwa organizacji,
   - przeprowadzenie analizy i szacowania ryzyka.

2. Charakterystyka działań realizowanych w ramach fazy zasadniczej cyklu życia Polityki Bezpieczeństwa Informacji

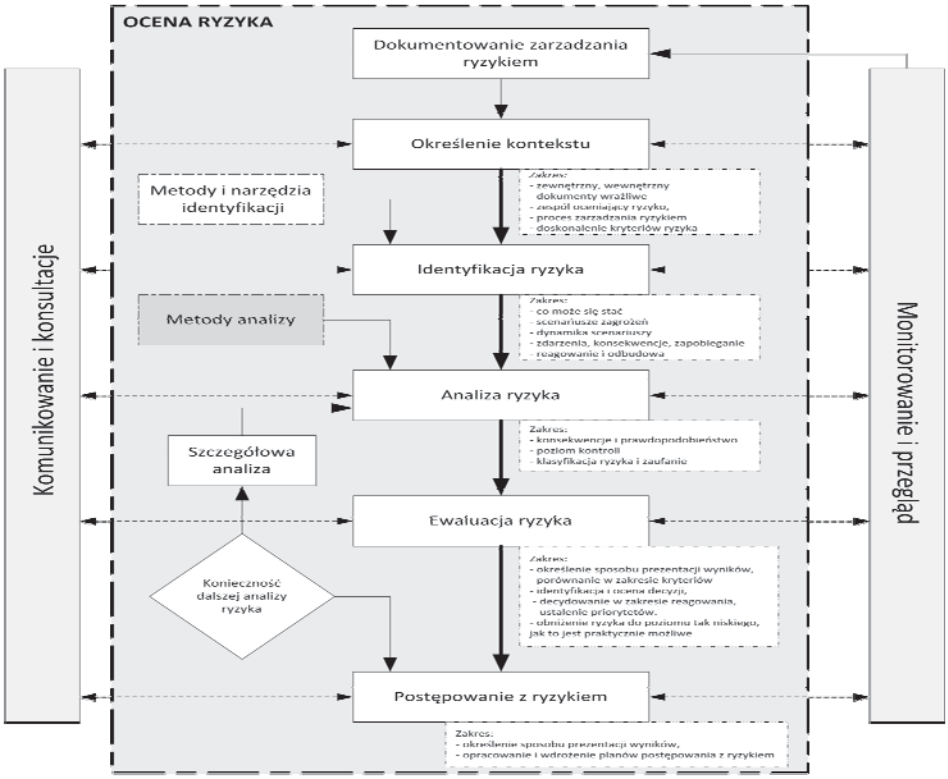
2.1. Audyt istniejących zasobów i zagrożeń

Audyt istniejących zasobów i zagrożeń to systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełniania/zachowania atrybutów bezpieczeństwa przez poszczególne aktywa (procesy i zasoby informacyjne) organizacji. Audyty tego typu, zwane często wewnętrznymi, to konieczny element systemowego zarządzania bezpieczeństwem informacji, a przy tym jeden z ważniejszych elementów stojących na straży utrzymania systemu i jego ciągłego doskonalenia. Czynności kontrolne audytu mają na celu porównanie stanu rzeczywistego ze stanem oczekiwanym określonych zasobów organizacji i wykazanie istniejących odchyleń. Jest to również proces zbierania i oceniania dowodów w celu określenia, czy system informacyjny i związane z nim zasoby lub procesy informacyjne właściwie są chronione, utrzymują integralność danych i dostarczają odpowiednich i rzetelnych informacji, osiągają efektywnie cele organizacji, oszczędnie wykorzystują zasoby procesów ochronnych i stosują mechanizmy kontroli wewnętrznej,

tak aby dostarczyć rozsądnego zapewnienia, że osiągane są cele operacyjne i kontrolne, oraz że chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane, a ich skutki na czas korygowane. Audyt w środowisku informatycznym powinien być niezależnym przeglądem aplikacji, systemu informatycznego i sieci do oceny zgodności z ustaloną polityką, przyjętymi wytycznymi oraz standardami. Wyniki audytu powinny być podstawą do działań prewencyjnych, zapobiegawczych lub wdrożenia stosownych mechanizmów zabezpieczeń. W ten sposób audyt może przyczynić się do uzyskania przez organizację wyższego poziomu bezpieczeństwa.

2.2. Przeprowadzenie analizy ryzyka

Analiza ryzyka to określone działania skierowane na obniżenie negatywnego wpływu ryzyka na funkcjonowanie organizacji i podejmowanie odpowiednich działań służących przeciwdziałaniu i ograniczaniu ryzyka. Pozwala na identyfikację, ocenę i monitorowanie poziomu ryzyka w sposób jakościowy i ilościowy. Przeprowadzenie analizy ryzyka sprowadza się do wskazania aktywów najbardziej zagrożonych w organizacji (miejsc o relatywnie wysokim prawdopodobieństwie zmaterializowania się zagrożenia), dzięki czemu wiemy, którymi aktywami należy się zająć w pierwszej kolejności i wdrożyć dla nich zabezpieczenia (fizyczne, techniczne lub organizacyjne). Wdrożenie zabezpieczeń może wiązać się z koniecznością przeznaczenia dodatkowych funduszy na ten cel. Analiza ryzyka powinna być przejrzysta i kompleksowa. Daje nam to gwarancję efektywnego i szybkiego wykrycia naruszenia bezpieczeństwa, czego efektem jest minimalizacja strat. Powinna być również dynamiczna, powtarzalna oraz cechować się reakcją na zmiany. Jest to szczególnie ważne, ponieważ ryzyka nieprzerwanie się zmieniają, ewoluują, powstają i zanikają. Na rysunku 2 zaprezentowano całościowy proces zarządzania ryzykiem, gdzie identyfikacja aktywów i analiza ryzyka są jego częścią (Stanik, Kiedrowicz, Hoffmann, 2017).



Rysunek 2. Przegląd procesu zarządzania ryzykiem w bezpieczeństwie informacji

Źródło: opracowanie własne.

2.3. Ustanowienie kontekstu bezpieczeństwa

Na tym etapie dokonuje się opracowania tzw. metodyki zarządzania ryzykiem, w której są określane wszystkie istotne zasady dotyczące całego procesu zapewniania bezpieczeństwa, w celu zapewnienia jego powtarzalności i zagwarantowania, że wyniki szacowania ryzyka są porównywalne na przestrzeni czasu. Na tym etapie określa się również odpowiedzialności w zakresie zarządzania ryzykiem, ze szczególnym uwzględnieniem roli kierownictwa w etapie określenia kryteriów akceptacji ryzyka. Kryteria brane pod uwagę to m.in.: ogólny stopień poufności, skutki utraty lub modyfikacji danego zasobu informacyjnego, koszt początkowy, koszt zastąpienia lub odtworzenia, wartość dobrego imienia organizacji itp. Zaleca się, aby kryteria stosowane jako podstawa do przypisywania wartości wszystkim zasobom informacyjnym były opisane za pomocą jednoznacznych określeń. Często jest to jeden z najtrudniejszych aspektów wartościowania zasobów, ponieważ wartości części zasobów mogą być określane subiektywnie i przeważnie takie wartościowanie wykonuje wiele różnych osób. Zaleca

się opracowanie zbioru kryteriów oceny ryzyka w bezpieczeństwie informacji w organizacji, z uwzględnieniem następujących czynników:

- strategicznej wartości biznesowych procesów informacyjnych,
- krytyczności zaangażowanych aktywów informacyjnych,
- wymagań prawnych,
- operacyjnej i biznesowej wagi dostępności, poufności i integralności,
- negatywnych następstw dla wizerunku i reputacji.

Dodatkowo, kryteria oceny ryzyka mogą być użyte do określenia priorytetów postępowania z ryzykiem.

2.4. Opracowanie projektu i dokumentacji PBI

Produktywne funkcjonowanie organizacji w znacznej mierze uzależnione jest od precyzyjnie zaplanowanej, przygotowanej oraz wdrożonej polityki bezpieczeństwa, szczegółowo definiującej szereg działań zabezpieczających podstawowe aktywa organizacji (procesy biznesowe, zasoby informacyjne) oraz krytyczne elementy infrastruktury IT zarówno pod kątem technicznym, jak i organizacyjnym. Bazowa polityka bezpieczeństwa wymaga ciągłych modyfikacji, odzwierciedlających zmieniające się wewnętrzne i zewnętrzne uwarunkowania pracy organizacji, profilu działania, stosowanych technologii informatycznych oraz oprogramowania. Należy określić, co jaki czas mają być wykonywane wewnętrzne i zewnętrzne audyty bezpieczeństwa oraz zmiany w polityce bezpieczeństwa informacji. W skład projektu bazowego dokumentu PB powinny wchodzić procedury podwyższające standard bezpieczeństwa organizacji, w tym procedury bezpiecznej eksploatacji systemu informacyjnego oraz rozwiązania kompatybilnego dostępu do sieci, zarządzania zasobami oraz skuteczne systemy zabezpieczeń. Ściśle określony oraz poprawnie sporządzony zbiór procedur bezpiecznej eksploatacji systemu informacyjnego oraz instrukcji postepowania jest nieodzowną metodą pozwalającą na efektywne wdrożenie polityki bezpieczeństwa w organizacji. Odpowiednio dobrana i skonstruowana polityka bezpieczeństwa informacji powinna więc kompleksowo chronić organizację zarówno od wewnątrz, jak i na zewnątrz organizacji. Opracowana polityka bezpieczeństwa powinna uwzględniać:

- analizę wszelkich zagrożeń i podatności zasobów informacyjnych oraz słabych punktów infrastruktury IT w organizacji,
- szczegółową charakterystykę zasad formułujących skuteczne zapewniane/zachowanie kluczowych atrybutów bezpieczeństwa w stosunku do podstawowych aktywów organizacji oraz prawidłowy dostęp i zarządzanie tymi aktywami w sieci,
- określenie procedur definiujących metody postępowania podczas naruszenia bezpieczeństwa,
- wdrożenie polityki bezpieczeństwa poprzez instruktaż pracowników danej organizacji.

2.5. Ciągły nadzór, kontrola i modyfikacja istniejącej polityki

Rozwój i doskonalenie Polityki Bezpieczeństwa Informacji jest pracą o charakterze ciągłym. W miarę upływu czasu pojawiają się nowe technologie informacyjne i związane z nimi zagrożenia. Ponadto dokonywane są zmiany w systemie informacyjnym oraz innych systemach funkcjonowania organizacji. Polityka bezpieczeństwa musi stale uwzględniać te nowe warunki i sytuacje – w przeciwnym przypadku staje się bezużyteczna. Dokument Polityki Bezpieczeństwa Informacji powinien być kreowany i doskonalony w oparciu o pewien zestaw reguł, który w najbardziej ogólnym kształcie powinien obejmować:

- określenie rodzaju procesów i zasobów informacyjnych, którymi dysponuje podmiot polityki bezpieczeństwa informacji oraz ustalenie, jak przedstawia się ich jakość i wielkość w stosunku do potrzeb,
- zorganizowanie (modyfikację) systemu zarządzania informacją obejmującego jej pozyskiwanie, gromadzenie, przetwarzanie, przechowywanie, przekazywanie i niszczenie,
- wydzielenie pakietów informacji wrażliwych (w tym informacji poufnych i tajemnic),
- określenie personalnej odpowiedzialności w zakresie zarządzania informacją, w tym także pakietami informacji wrażliwej,
- informowanie zainteresowanych stron o działaniach i udoskonaleniach.

2.6. Wdrożenie projektu bazowej polityki bezpieczeństwa

2.6.1. Proces opracowywania strategii zabezpieczeń

Skuteczna ochrona zasobów informacyjnych organizacji wymaga stosowania różnego rodzaju zabezpieczeń, w tym wprowadzenia kilku zabezpieczeń jednocześnie. Niemniej nie należy wprowadzać zabezpieczeń, jeśli poziom ryzyka jest akceptowalny, nawet wtedy, jeśli istnieją podatności, gdyż nie są znane zagrożenia, które te podatności mogłyby wykorzystać. Wszystkie te ograniczenia determinują wybór konkretnych zabezpieczeń (Stanik, Napiórkowski, Hoffmann, 2016). Przykładowe etapy Strategii Zabezpieczeń zilustrujowano w tabeli 1.

Bezpieczeństwo informacyjne nie powinno być traktowane jako rozwiązanie o charakterze czysto technicznym, gdyż bez wsparcia właściwego zarządzania i procedur może okazać się nieskuteczne. Implementacja zabezpieczeń może być trudna do realizacji i kosztowna. Dobrą praktyką jest stosowanie różnych kombinacji zabezpieczeń zarówno organizacyjnych, jak i technicznych.

Tabela 1. Specyfikacja faz i zakres działania w ramach strategii zabezpieczeń

Nazwa fazy	Opis działań
Zrozumienie obecnej sytuacji	Rozpoczyna się od bieżącej oceny poziomu zabezpieczeń istniejących w organizacji. Dokonuje się przeglądu wykorzystanych technologii przez instytucje, jej polityk, procedur oraz dyrektyw. Wykonuje się ocenę ryzyka przy użyciu technik i narzędzi, które testują siłę obecnych mechanizmów zabezpieczeń. W tej fazie należy jasno określić obszary, które są wykluczone ze sfery zabezpieczeń
Zdefiniowanie środowiska najbardziej pożądanego	Dokonuje się przeglądu najlepszych polityk, procedur i działań praktycznych. Przeprowadza się rozmowy i wywiady z jak największą liczbą osób, z uwzględnieniem specjalistów technik informatycznych. Na podstawie analizy wymagań tworzy się architekturę zabezpieczeń
Ocena alternatywnych rozwiązań	Dokonuje się przeglądu potencjalnych aplikacji i kierunków rozwoju technik informatycznych
Określenie najlepszej procedury postępowania	W tej fazie prezentowane są zalecenia szczegółowych rozwiązań i procesów działań. Analizie poddaje się ryzyko oraz koszty, a także opracowuje plan taktyczny
Rozpoczęcie	W tej fazie następuje wykonanie planu oraz wdrożenie rekomendowanych rozwiązań technologicznych i proceduralnych

Źródło: opracowano na podstawie Wikipedii.

2.6.2. Proces projektowania, wdrażania i doskonalenia zabezpieczeń

Cele stosowania zabezpieczeń i zabezpieczenia powinny być dobierane na podstawie:

- zapisów obowiązujących aktów prawnych,
- wyników przeprowadzonej analizy ryzyka w bezpieczeństwie informacji,
- wyników przeprowadzonych audytów,
- dobrych praktyk uznanych w obrocie profesjonalnym.

W doborze celów stosowania zabezpieczeń i zabezpieczeń należy brać pod uwagę zalecenia wynikające z Polskiej Normy PN-ISO/IEC 27002. Cele zabezpieczeń i zabezpieczenia powinny być zawarte w Deklaracji Stosowania zabezpieczeń Organizacji. W procesie projektowania zabezpieczeń należy uwzględnić:

- typ działalności biznesowej,
- przepisy prawne dotyczące: ochrony danych osobowych, własności intelektualnej, Krajowych Ram Interoperacyjności i minimalnych wymagań dla systemów teleinformatycznych oraz Politykę Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej,
- ilość przetwarzanej informacji, ilość i typ informacji wrażliwych,
- liczbę platform technologicznych (informatycznych) oraz liczbę eksploatowanych systemów informacyjnych (w tym systemów krytycznych) i ich złożoność (systemy informatyczne, sieci).

W związku ze stale zmieniającymi się warunkami zewnętrznymi zachodzi konieczność modyfikacji/doskonalenia zabezpieczeń, co wymusza stosowanie monitorowania i oceny skuteczności zabezpieczeń zarówno organizacyjnych, jak i technicznych,

identyfikacji ryzyka i opracowania zasad postepowania z ryzkiem, wdrożenia zmodyfikowanych zabezpieczeń.

Wybór konkretnych zabezpieczeń powinien być uwarunkowany ryzykiem związanym z bezpieczeństwem kluczowych procesów biznesowych, informacji oraz ogólnym podejściem do zarządzania ryzykiem w danej organizacji. Uwzględniając specyfikę organizacji, można wyłączyć pewne zabezpieczenia. Jednakże każde wyłączenie ze zbioru wymaganych zabezpieczeń określonych w normie ISO/IEC 27001 wymaga szczegółowego uzasadnienia. Zdefiniowane zabezpieczenia uznane jako najlepsze praktyki są na tyle uniwersalne, że można je wprost zastosować w organizacjach różnych wielkości, wielu lokalizacji i złożoności struktury organizacyjnej.

2.7. Proces oceny jakości wprowadzonych zabezpieczeń

Na proces oceny jakości zabezpieczeń składają się dwa typy działań (Stanik, Protasowicki, 2015):

- testowanie zabezpieczeń,
- ocena skuteczności zabezpieczeń.

2.7.1. Testowanie zabezpieczeń

Testowanie zabezpieczeń polega na zbieraniu dowodów audytowych. W oparciu o zapisy z audytu można stwierdzić, na ile skuteczne są zabezpieczenia. Dowody audytowe są zbierane poprzez wykorzystanie różnych metod i technik, np. kontrolę wzrokową, wywiady z pracownikami (znajomość procedur i świadomość zastosowanych zabezpieczeń), testowanie zasobu/systemu w odniesieniu do zabezpieczeń technicznych, np. sprawdzenie ustawień konfiguracyjnych systemów, sprawdzenie podatności aplikacji za pomocą specjalistycznego oprogramowania.

Kontrola wzrokowa oznacza, że zabezpieczenia te zwykle wymagają kontroli wzrokowej na miejscu w celu oceny ich skuteczności. Obserwacje audytorów mają na celu potwierdzenie istnienia zabezpieczeń. Wywiady (rozmowy) z pracownikami powinny potwierdzić znajomość procedur i świadomość pracowników w zakresie stosowanych zabezpieczeń organizacyjnych. Przykładowy wykaz zabezpieczeń, które mogą podlegać testowaniu podczas audytu ze wskazaniem sposobu ich testowania, zawarto w tabeli 2.

Zastosowane metodyki testowania zabezpieczeń przeważnie są rozwiązaniami autorskimi, które powinny być zweryfikowane podczas prowadzonych audytów wstępnych bezpieczeństwa. W ramach gromadzenia dowodów audytowych, zwłaszcza podczas testowania zabezpieczeń systemu, należy mieć pewność co do zrozumienia przez audytora wymagań w odniesieniu do zagadnień prawa własności intelektualnej, ochrony danych osobowych, regulacji dotyczących zabezpieczeń kryptograficznych, podpisów elektronicznych i cyfrowych, cyberprzestępczości, gromadzenia elektronicznych materiałów dowodowych, testów penetracyjnych.

Tabela 2. Wykaz testowanych zabezpieczeń – przykład

Nazwa zabezpieczenia	Metodyka testowania
Kopie zapasowe informacji	analiza procedury wykonywania kopii zapasowych; próba odtworzenia danych systemowych z kopii zapasowych
Rejestrowanie zdarzeń	zbadanie dostępu do dziennika zdarzeń; analiza rejestru działań administratorów i operatorów
Procedura nadawania i odbierania uprawnień	sprawdzenie nadania i odebrania dostępu do systemu informatycznego; zbadanie czy w systemie informatycznym odnotowano odebranie praw dostępu pracownikowi i użytkownikowi zewnętrznemu po zakończeniu pracy
Polityka używania zabezpieczeń kryptograf	zbadanie parametrów certyfikatu domeny ze szczególnym uwzględnieniem ważności certyfikatu i zastosowanej funkcji skrótu

Źródło: opracowanie własne.

2.7.2. Ocena skuteczności zabezpieczeń

Ocena skuteczności zabezpieczeń jest funkcją/pochodną zastosowanej metody pomiarowej, przyjętych miar oraz specyfiki danej organizacji (Krawiec, 2013). Czynności dotyczące określenia miar i metod pomiarowych powinny być uzależnione od zasobów kadrowych, infrastrukturalnych i finansowych, powinny również dotyczyć wyboru obiektu pomiarowego i jego atrybutów, wyboru metody pomiarowej, określenia zakresu pomiarowego, ustalenia sposobu gromadzenia danych i ich analizy, opracowania dokumentacji pomiarowej. Zakres czynności pomiarowych może być zawężony do aktywów szczególnie chronionych (najwyższy priorytet). Zakres pomiarowy powinni określić interesariusze.

Metody pomiarowe można podzielić na obiektywne i subiektywne. W metodach obiektywnych wykorzystuje się kryteria liczbowe (np. obliczanie za pomocą formuły matematycznej), które mogą być realizowane w sposób automatyczny lub ręczny. Metoda subiektywna to sposób oceny realizowany przez człowieka na podstawie własnego doświadczenia.

Ważne jest, aby opracować i wdrożyć procedury gromadzenia i analizowania danych oraz raporty z wynikami pomiarów. Procedury te powinny dotyczyć także narzędzi pomiarowych oraz technik pomiaru. Wyniki pomiarów powinny być oceniane pod kątem przydatności w odniesieniu do potrzeb informacyjnych.

Podsumowanie

Podstawowymi źródłami kreowania polityki bezpieczeństwa w sferze informacyjnej organizacji powinny być: wyniki z prac przygotowawczych, wyniki diagnozy przedwdrożeniowej SZBI, wyniki z procesu analizy i szacowania ryzyka oraz zapisy z realizacji audytów wewnętrznych bezpieczeństwa.

Zakres prac przygotowawczych i jakość otrzymanych wyników bardzo silnie wpływają na zakres i wybór metodyki realizacji działań zasadniczych, a w szczególności na sposób przebiegu procesu analizy ryzyka i użyteczności jego wyników.

Do zbioru prac przygotowawczych najczęściej należą: analiza SWOT, audyt wstępny lub wewnętrzny systemu informacyjnego na potrzeby bezpieczeństwa informacji organizacji, diagnoza zasobów informacyjnych i zagrożeń, identyfikowanie, klasyfikowanie i wartościowanie aktywów organizacji.

Na opracowanie polityki bezpieczeństwa składa się szereg czynności, z których można skonstruować rożne modele cyklu życia, metodyki lub podejścia tworzenia dokumentu polityki bezpieczeństwa.

Dokument określający politykę bezpieczeństwa informacji nie powinien mieć charakteru zbyt abstrakcyjnego. Decydując się na opracowanie, wdrożenie, użytkowanie i doskonalenie polityki bezpieczeństwa powinniśmy opierać się przede wszystkim o wyniki analizy ryzyka, a ponadto brać pod uwagę wyniki przeprowadzonych audytów, zbiór „dobrych" praktyk z zakresu bezpieczeństwa informacyjnego, wytyczne zawarte w dokumentach standaryzujących, zalecenia i porady fachowców lub ekspertów z dziedziny bezpieczeństwa informacji.

Przy projektowaniu polityki bezpieczeństwa należy rozważyć, czy organizacja będzie w stanie ponieść koszty wprowadzania tej polityki w życie. Podwyższanie poziomu bezpieczeństwa organizacji odbywa się najczęściej kosztem wygody i efektywności działania. Dlatego, opierając się na zalecanych modelach czy standardach w tej dziedzinie, należy pamiętać o dostosowaniu rozwiązania do specyfiki organizacji, tak aby nadać jej cechy ułatwiające zastosowanie w praktyce.

Rozwój i doskonalenie polityki bezpieczeństwa jest pracą o charakterze ciągłym. W miarę upływu czasu pojawiają się nowe zagrożenia oraz dokonywane są zmiany w systemie informacyjnym organizacji (nowe technologie, rotacja pracowników itp.). Polityka bezpieczeństwa musi stale uwzględniać nowe warunki – w przeciwnym przypadku staje się bezużyteczna.

Literatura

http://www.faqs.org/rfcs/rfc2196.html (6.12.2017).

http://www.itl.nist.gov/ fipspubs/ fip191.htm (6.12.2017Krawiec, J. (2013). Systemy SZBI – Pomiary bezpieczeństwa informacji. *IT Professional*, *6*.

Norma PN-ISO/IEC27001:2014-12 (2014). *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.*

ISO/IEC 27002 – *Praktyczne zasady zabezpieczania informacji*.

RFC 2196 (1997). *Site Security Handbook.*

FIPS PUB 191 (1994). *Federal Information Processing Standards Publication 191*. Standard for: Guideline for the Analysis of Local Area Network Security.

Stanik, J., Kiedrowicz, M. (2017). Model ryzyka procesów biznesowych. *Ekonomiczne Problemy Usług*, *1* (126, t. 1), 325–338.

Stanik, J. Kiedrowicz, M., Hoffmann, R. (2017). Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych. *Ekonomiczne Problemy Usług*, *1* (126, t. 1), 339–354.

Stanik, J., Napiórkowski, J., Hoffmann, R. (2016). Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji. *Ekonomiczne Problemy Usług*, *123*, 321–336.

Stanik, J., Protasowicki, T. (2015). *Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego*. KKIO „Od procesów do oprogramowania: badania i praktyka". Pobrano z: http://eurlex.europa.eu/legalcontent/PL/TXT/HTML/?uri=CELEX:32016R0679&qid=1495623691523&from=en (8.01.2018).

http://www.faqs.org/rfcs/rfc2196.html (6.12.2017).

http://www.itl.nist.gov/ fipspubs/ fip191.htm (6.12.2017).

RISK ANALYSIS REPORT AS A KEY ELEMENT OF THE CREATION OF INFORMATION SECURITY POLICY – INDIVIDUAL ASPECT

Keywords: information security, security policy, risk analysis

Summary. The authors present a proprietary approach to the process of creating and maintaining an information security policy in the organization. The proposed method of creating the Security Policy is comprehensive and easy to apply in practice. It is based on a life cycle of a security policy whose start-up phase is preparatory work carried out quite rarely and on demand, while the regular stage is work performed cyclically – the PDCA model. Within each cycle, the following processes are performed: risk analysis, preparation of the Basic Information Security Policy (BPBI) project, project implementation, development of a security strategy, assessment of the effectiveness of the implemented strategy, improvement of the security policy.

Translated by Maciej Kiedrowicz

Cytowanie

Stanik, J., Kiedrowicz, M. (2018). Raport analizy ryzyka jako kluczowy element tworzenia polityki bezpieczeństwa informacji. *Ekonomiczne Problemy Usług*, *2* (131/1), 347–360. DOI: 10.18276/epu.2018.131/1-34.