© Wydawnictwo UR 2018 „Edukacja – Technika – Informatyka" nr 2/24/2018
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2018.2.5

JERZY KRAWIEC

Badanie skuteczności systemu zarządzania bezpieczeństwem informacji

Testing the Effectiveness of an Information Security Management System

Doktor inżynier, Politechnika Warszawska, Wydział Inżynierii Produkcji, Instytut Organizacji Systemów Produkcyjnych, Zakład Systemów Informatycznych, Polska

Streszczenie

W artykule przedstawiono problematykę dotyczącą ewaluacji skuteczności zabezpieczeń systemu zarządzania bezpieczeństwem informacji. Zdefiniowano cele pomiaru oraz zaproponowano model pomiarowy do oceny skuteczności zabezpieczeń systemu. Na podstawie przyjętego modelu pomiarowego określono przykładowe wskaźniki pomiarowe, które mogą być zastosowane do badania skuteczności wdrożonych zabezpieczeń. Zaprezentowano wnioski dotyczące wdrażania systemu zarządzania bezpieczeństwem informacji.

Słowa kluczowe: system zarządzania, bezpieczeństwo informacji, pomiary, zabezpieczenia

Abstract

Problems regarding the evaluation of the effectiveness of the information security management system have been presented. Measurement goals have been defined and a measurement model has been proposed to assess the effectiveness of system security. Based on the proposed measurement model, exemplary measurement indicators have been determined that can be used to test the effectiveness of the implemented security controls. Conclusions regarding the implementation of the information security management system have been presented.

Keywords: management system**,** information security, measurements, controls

Wstęp

Systemy wspierające zarządzanie informacją są ważnymi aktywami każdej instytucji. Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji jest niezbędne dla utrzymania pozycji rynkowej, zachowania płynności finansowej, spełnienia wymagań prawnych czy wizerunku instytucji. Podejmowanie decyzji w coraz bardziej skomplikowanym otoczeniu biznesowym wymaga posiadania wiarygodnej i kompletnej informacji. Zatem kluczowym problemem staje się

zarządzanie tą informacją, a dokładniej jej bezpieczeństwem. Podejmowanie decyzji w dzisiejszym otoczeniu biznesowym wymaga posiadania wiarygodnej i kompletnej informacji. „Jeżeli nie możesz czegoś zmierzyć, nie możesz tym zarządzać". Ta maksyma, zgodnie z metodą BSC (*Balanced Score Card*), nabiera szczególnego znaczenia w działalności każdej instytucji.

Celem artykułu jest przedstawienie metod badań skuteczności zabezpieczeń systemu zarządzania bezpieczeństwem informacji.

Głównym problemem badawczym jest sposób pomiaru poziomu bezpieczeństwa informacji i na tej podstawie określenie skuteczności zastosowanych zabezpieczeń systemu zarządzania bezpieczeństwem informacji.

Hipoteza badawcza brzmi: za pomocą odpowiedniej metody pomiarowej oraz właściwemu zdefiniowaniu wskaźników pomiarowych można określać skuteczność stosowanych zabezpieczeń systemu zarządzania bezpieczeństwem informacji.

Zasoby informacyjne

Zasoby to wszystkie aktywa, pracownicy i ich umiejętności, technologia, pomieszczenia, materiały oraz informacje, do których organizacja (instytucja) musi mieć dostęp, aby realizować swoje cele. Zasoby informacyjne to informacje (w postaci elektronicznej i nieelektronicznej). Z informacjami ściśle związane są dane, które niewłaściwie są traktowane jako synonimy informacji.

Informacja, w przetwarzaniu informacji, to wiedza obejmująca: fakty, zdarzenia, przedmioty, procesy lub idee, zawierająca koncepcje, która w ustalonym kontekście ma określone znaczenie. Natomiast w teorii informacji informacja oznacza wiedzę redukującą lub usuwającą niepewność dotyczącą wystąpienia określonego zdarzenia z danego zbioru zdarzeń możliwych (ISO/IEC 2382, 2015).

Dane to reprezentacja informacji przedstawiona w sposób sformalizowany, dogodny do komunikowania się, interpretowania, przechowywania lub przetwarzana w pamięci (człowieka lub komputera). W kontekście pomiarów w zarządzaniu bezpieczeństwem informacji dane to także zbiór wartości przyporządkowanych do miar bazowych, miar pochodnych oraz wskaźników (ISO/IEC 2382, 2015).

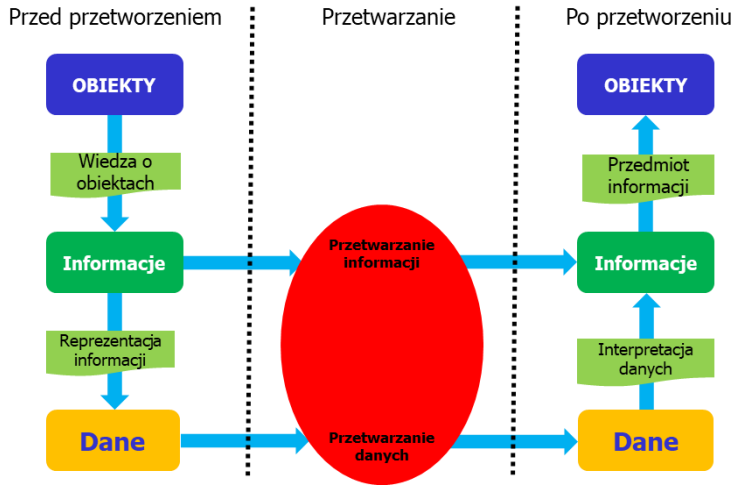
Zarówno informacje, jak i dane mogą być przetwarzane przez systemy informatyczne lub przez ludzi.

Przetwarzanie informacji to uporządkowane wykonywanie operacji na informacji, które obejmuje przetwarzanie danych i może również obejmować operacje przesyłania danych i automatyzacji prac biurowych (ISO/IEC 2382, 2015).

Przetwarzanie danych to usystematyzowane wykonywanie operacji na danych, w tym uporządkowane wykonywanie operacji, np. operacje arytmetyczne lub operacje logiczne na danych, łączenie i sortowanie danych, asemblowanie lub kompilowanie programów, operacje na tekście: redagowanie, sortowanie,

łączenie, zapamiętywanie, wyszukiwanie, wyświetlanie lub drukowanie (ISO/IEC 2382, 2015).

Relacje między informacjami a danymi w różnych fazach przetwarzania przedstawiono na rys. 1.



Rysunek 1. Relacje między informacjami a danymi

Źródło: opracowanie własne na podstawie: ISO/IEC 2382 (2016).

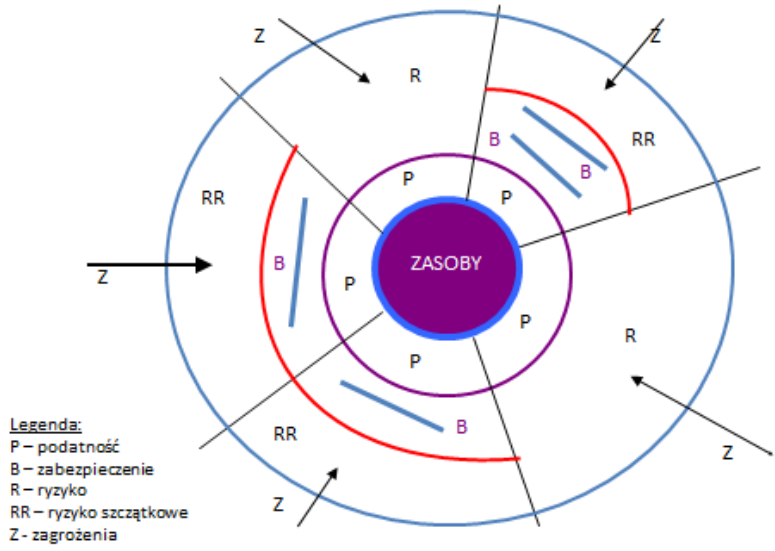
Jak wynika rys. 1, pojęcia *informacje* i *dane* nie są synonimami. Najogólniej można powiedzieć, że przed przetworzeniem dane to reprezentacja informacji, a po przetworzeniu informacje są interpretacją danych.

Ogólny model bezpieczeństwa informacji

W dostępnych źródłach, zwłaszcza internetowych, można spotkać wiele modeli bezpieczeństwa informacji. Jednak najbardziej przejrzysty wydaje się model opisany w normach międzynarodowych, co przedstawiono na rys. 2.

Bezpieczeństwo informacji bazuje na trzech podstawowych atrybutach: poufności, integralności i dostępności (ISO/IEC 27000, 2016). Poufność to cecha polegająca na nieudostępnianiu lub nieujawnianiu informacji nieautoryzowanym osobom, podmiotom lub procesom. Integralność to właściwość zapewniająca dokładność i kompletność aktywów. Dostępność to zapewnienie użyteczności informacji na żądanie autoryzowanego podmiotu.

Atrybutami pomocniczymi w modelu bezpieczeństwa informacji są: autentyczność (podmiot jest tym, za kogo się podaje), rozliczalność (odpowiedzialność podmiotu za jego akcje i decyzje), niezaprzeczalność (zdolność udowodnienia deklarowanych zdarzeń lub działań) i niezawodność (cecha oznaczająca spójne, zamierzone, zachowanie i skutki).



Rysunek 2. Ogólny model bezpieczeństwa informacji

Źródło: opracowanie własne na podstawie: ISO/IEC 27000 (2016).

Systemy informatyczne są narażone na zagrożenia pochodzące z wielu źródeł, zarówno zewnętrznych, jak i wewnętrznych. Najogólniej można podzielić zagrożenia na zależne od człowieka (świadome, przypadkowe) oraz niezależne (środowiskowe) (Górny, Krawiec, 2016).

Zagrożenia stają się coraz bardziej wyrafinowane i przysparzają znacznych strat w wymiarze materialnym i niematerialnym. Bezpieczeństwo informacji poprzez minimalizację ryzyka w działalności biznesowej i ochronie infrastruktury krytycznej jest ważne zarówno dla sektora publicznego, jak i komercyjnego. Zatem podstawą bezpieczeństwa informacji powinny być zabezpieczenia, czyli procedury bezpieczeństwa, wspierane przez środki techniczne (Krawiec, 2017).

Zabezpieczenia mogą być skuteczne, jeśli ryzyko związane z zagrożeniami lub podatnościami będzie zminimalizowane. Sprowadzenie ryzyka do poziomu akceptowalnego może czasami wymagać wprowadzenia kilku zabezpieczeń. Nie wprowadza się zabezpieczeń, jeśli poziom ryzyka jest akceptowalny, nawet jeśli istnieją podatności, gdyż nie są znane zagrożenia, które te podatności mogłyby wykorzystać. Wszystkie te ograniczenia determinują wybór konkretnych zabezpieczeń.

System zarządzania bezpieczeństwem informacji

Zapewnienie bezpieczeństwa informacji na odpowiednim poziomie może być realizowane jedynie przez rozwiązanie systemowe, czyli System Zarządzania Bezpieczeństwem Informacji (SZBI). Wdrażanie takiego systemu powinno być poprzedzone analizą ryzyka oraz klasyfikacją zasobów instytucji. Na tej

podstawie dokonujemy wyboru konkretnych zabezpieczeń, zarówno organizacyjnych, jak i technicznych. Z prawnego punktu widzenia najważniejsze są zabezpieczenia dotyczące ochrony danych osobowych, tajemnicy przedsiębiorstwa oraz ochrony własności intelektualnej. Za powszechną praktykę w zakresie bezpieczeństwa informacji są uznawane zabezpieczenia obejmujące (ISO/IEC 27001, 2013):

- politykę bezpieczeństwa informacji,
- przypisanie kompetencji w zakresie bezpieczeństwa informacji,
- uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji,
- właściwą obsługę aplikacji przetwarzających dane,
- zarządzanie podatnościami technicznymi,
- zarządzanie ciągłością działania,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- ciągłe doskonalenie SZBI.

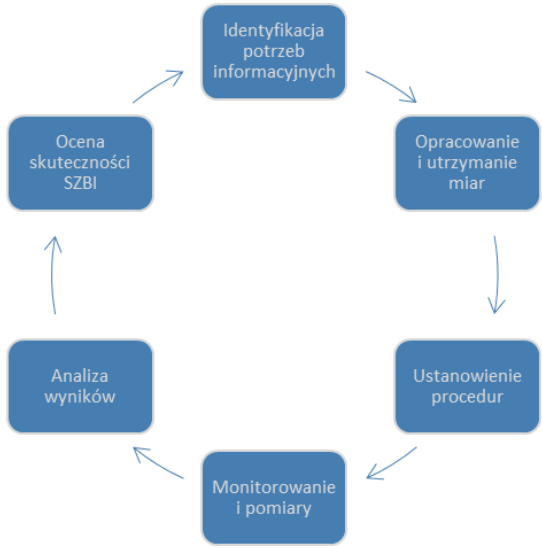
Zasady wyboru zabezpieczeń traktujemy jako wytyczne do opracowania własnych zabezpieczeń, zarówno organizacyjnych, jak i technicznych, uwzględniających specyfikę instytucji. Nie wszystkie zabezpieczenia i zalecenia mogą mieć zastosowanie.

W procesie wdrażanie SZBI należy uwzględnić zasadę obejmującą takie cechy, jak: przydatność, adekwatność i skuteczność. Przydatność powinna wynikać np. z konieczności – uwarunkowań prawnych lub biznesowych. Adekwatność polega na dobraniu odpowiednich środków ochrony (zabezpieczeń) do chronionych zasobów. W tym przypadku kluczowa jest prawidłowa klasyfikacja informacji. System Zarządzania Bezpieczeństwem Informacji musi być skuteczny, aby dostatecznie uzasadniał interes biznesowy oraz spełnianie wymagań prawnych (Krawiec, Ożarek, 2014).

Pomiary skuteczności zabezpieczeń systemu

Skuteczność systemu powinna być mierzona tak, aby ocena była obiektywna. Nie można wprost zmierzyć bezpieczeństwa informacji, zatem potrzebne są mierniki (wskaźniki).

W celu uzyskania porównywalnych i powtarzalnych wyników należy określić sposób pomiaru skuteczności zabezpieczeń (ISO/IEC 27004, 2106). Spełnienie wymagań dotyczących pomiarów SZBI zależy od kilku istotnych czynników: zagrożeń, przed którymi staje instytucja, wielkości instytucji, dostępnych środków oraz uwarunkowań prawnych i kontraktowych. Staranny dobór metody pomiaru i uzasadnienie jej zastosowania mają zasadnicze znaczenie przy zapewnieniu adekwatności używanych zasobów. Pomiary powinny być integralną częścią prowadzenia działalności biznesowej. Na rys. 3 przedstawiono procesy monitorowania, pomiarów, analizy i oceny skuteczności zabezpieczeń SZBI.



Rysunek 3. Procesy pomiarowe

Źródło: opracowanie własne na podstawie: ISO/IEC 27004 (2016).

Określenie miar powinno rozpocząć się od zidentyfikowania potrzeb informacyjnych, aby zrozumieć cechy operacyjne i wydajność każdego aspektu SZBI. Instytucja powinna opracować miary, a następnie je aktualizować w zaplanowanych odstępach czasu lub gdy SZBI ulegnie istotnym zmianom. Ustanowienie procedur ma na celu zbieranie danych, ich bezpieczne przechowywanie, weryfikację, analizę oraz sporządzanie raportów dotyczących miar. Należy określić procedury monitorowania i pomiaru oraz przechowywania i weryfikacji. Kwalifikowanie danych w ramach etapu weryfikacji danych można przeprowadzać, stosując np. listę kontrolną, co powinno zapewnić, że wpływ brakujących danych na wiarygodność wyników analizy jest minimalny. Zebrane dane powinny być poddane analizie statystycznej w stosunku do każdego działania. Analiza danych powinna umożliwić określenie różnic między rzeczywistymi a oczekiwanymi wynikami pomiarów. W ramach ewaluacji należy zinterpretować dane w celu oceny skuteczności zastosowanych zabezpieczeń. Procesy monitorowania, pomiaru, analizy i oceny powinny być stale doskonalone, aby prawidłowo ocenić skuteczność stosowanych zabezpieczeń.

Miarą oszacowania lub oceny wartości atrybutów na podstawie modelu analitycznego w odniesieniu do określonych potrzeb informacyjnych jest wskaźnik. Zdefiniowanie wskaźnika odbywa się na podstawie wybranego modelu analitycznego stosowanego do miar bazowych i pochodnych w kontekście kryteriów decyzji. Wartości przypisane wskaźnikom powstają przez sumowanie wartości przypisanych miarom pochodnym i interpretacji tych wartości na podstawie

kryteriów decyzji. Każdy wskaźnik powinien mieć zdefiniowany format prezentacji jako część formatu raportu (sprawozdania). Format prezentacji wskaźnika powinien być dostosowany do potrzeb informacyjnych.

W tab. 1 przedstawiono wskaźniki pomiarowe do badania skuteczności zabezpieczeń systemu wdrożonego w instytucji publicznej, ale prowadzącej także działalność biznesową.

Tabela 1. Wskaźniki SZBI

Nazwa wskaźnika	Funkcja obliczenia wartości wskaźnika	Metoda pomiaru/ Źródło danych	Jednostka miary	Wartość wskaźnika	Zakres wskaźnika	Częstość pomiaru
Podatność aplikacji webowych (P)	$P = L_{wp}$ L_{wp} – Liczba wykrytych podatności aplikacji webowych systemów krytycznych	Testy penetracyjne wg OWASP Top 10	-	= 0 n/d ≥ 1	(0 – 10)	Raz na miesiąc
Jakość haseł (J)	$J = \frac{H_n}{H}$ H_n – Liczba haseł niezłamanych H – Liczba haseł ogółem	Atak hybrydowy	-	= 1 ≥ 0,9 < 0,9	(0 – 1)	Raz na miesiąc
Skuteczność zarządzania incydentami (S)	$S = L_{wi}$ L_{wi} - Liczba zidentyfikowanych incydentów	Dziennik incydentów	-	= 0 ≤ 10 > 10	(0 – ∞)	Raz na miesiąc
Przegląd logów (L)	$L = \frac{L_{pl}}{L_l}$ L_{pl} – Liczba przejrzanych plików logów L_l – Liczba plików logów ogółem	Dziennik przeglądanych plików logów	-	≥ 0,5 ≥ 0,2 < 0,2	(0 – 1)	Raz na miesiąc

Oznaczenia: n/d – nie dotyczy

Wartość wskaźników oznaczono kolorami (odpowiednio):

– zielonym – wartość wymagana, żadne działania nie są wymagane,
– żółtym – wartość akceptowalna, obserwacja i ewentualne działania zapobiegawcze,
– czerwonym – wartość niedopuszczalna, wymagane jest wprowadzenie działań korygujących.

W przypadku wartości akceptowalnej należy przyjąć taką wartość, która powinna się różnić od wartości wymaganej nie więcej niż o wartość ustaloną, np. może to być 10% od wartości wymaganej.

Źródło: opracowanie własne.

Podsumowanie

Ocena skuteczności zabezpieczeń jest funkcją zastosowanych miar (bazowych i pochodnych), wskaźników, metody pomiarowej oraz specyfiki danej instytucji.

Skuteczność realizacji programu pomiarowego zależy od działań realizowanych w określonym czasie obejmujących zapewnienie zgodności z programem, zapewnienie spójności pomiaru oraz adresowanie zmian w SZBI i jego otoczeniu (przepisy, wymagania, techniki pomiarowe).

Pomiary bezpieczeństwa informacji powinny być związane z szacowaniem i monitorowaniem ryzyka wynikającego z wykorzystania infrastruktury informatycznej w aspekcie zapewnienia poufności, dostępności i integralności informacji. Możliwość zapewnienia ww. atrybutów informacji zmusza do opracowywania metod pomiaru bezpieczeństwa i monitorowania zagrożeń. O wyborze wskaźników bezpieczeństwa informacji i ich wartości (wymaganych i akceptowalnych) powinno decydować kierownictwo firmy przy uwzględnieniu stanowiska osób doświadczonych w zakresie pomiarów bezpieczeństwa informacji.

Literatura

Górny, P., Krawiec, J. (2016). Cyberbezpieczeństwo – podejście systemowe. *Kwartalnik Obronność. Zeszyty Naukowe, 2* (18), 75–89.

ISO/IEC 2382 (2015). *Information Technology – Vocabulary*. Geneva.

ISO/IEC 27000 (2016). *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*. Geneva.

ISO/IEC 27001 (2013). *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, Geneva.

ISO/IEC 27004 (2016). *Information technology – Security Techniques – Information Security Management – Monitoring, Measurement, Analysis and Evaluation*. Geneva.

Krawiec, J. (2017). System zarządzania bezpieczeństwem informacji – zabezpieczenia. *Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, 1* (38), 46–59.

Krawiec, J., Ożarek, G. (2014). *System zarządzania bezpieczeństwem informacji w praktyce – zabezpieczenia*. Warszawa: PKN.