UNIWERSYTET Andrzeja Frycza Modrzewskiego w Krakowie

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2025
Nr 1 (LVIII)

https://doi.org/10.48269/2451-0718-btip-2025-1-004
Data wpłynięcia: 24.02.2025
Data akceptacji: 28.05.2025

Rola systemu zarządzania bezpieczeństwem informacji w budowaniu rezyliencji biznesowej przedsiębiorstwa

Krzysztof Łusiakowski

mgr, Politechnika Świętokrzyska w Kielcach
https://orcid.org/0009-0001-5770-2949

Wprowadzenie

Zapewnienie bezpieczeństwa informacji stanowi jedno z kluczowych wyzwań dla przedsiębiorstw w dobie gwałtownego rozwoju informatyzacji. Zarządzający przedsiębiorstwami zobowiązani są podejmować działania mające na celu ochronę aktywów informacyjnych przedsiębiorstwa. Ich uwaga powinna skupiać się na efektywnym wdrożeniu systemu bezpieczeństwa informacji, który zapewni kompleksową ochronę zasobów informacyjnych przedsiębiorstwa.

Bezpieczeństwo informacji to już nie tylko norma i wymóg czasów, ale obowiązek każdej organizacji będącej w posiadaniu informacji. Świadomość roli i znaczenia informacji w społeczeństwie informacyjnym sprawia, że kluczową kwestią staje się budowanie systemu jej bezpieczeństwa[1].

Współczesne przedsiębiorstwa funkcjonują w warunkach silnej turbulencji otoczenia. Skutki tej turbulencji przejawiają się w postaci możliwych kryzysów

[1] D. Fleszer, *Wokół problematyki bezpieczeństwa informacji*, „Rocznik Administracji i Prawa" 2018, t. 1, nr XVIII, s. 188, https://doi.org/10.5604/01.3001.0012.5998.

przedsiębiorstw, zarówno o charakterze ekonomicznym (m.in. w wyniku zawirowań na rynkach finansowych czy recesji), jak i pozaekonomicznym (wywoływanych przez wojny, katastrofy naturalne, terroryzm, skutki globalnego ocieplenia, pandemie itd.). Narastanie zjawisk o charakterze globalnym (pandemie, katastrofalne zjawiska naturalne, np. huragany, susze i trzęsienia ziemi) powoduje, że podmioty gospodarcze powinny wykazywać się zdolnościami o charakterze rezylientnym – zapewniać sobie przetrwanie poprzez dostosowywanie się (na ile to możliwe) do występujących zmian[2]. Rezyliencja musi odnosić się również do pojawiających się naruszeń bezpieczeństwa informacji, masowych ataków na przedsiębiorstwo, kradzieży danych i innych cyberprzestępstw.

Kadra zarządzająca powinna zdawać sobie sprawę z istotnej roli bezpieczeństwa informacji w realizacji strategii przedsiębiorstwa. Osiąganie wyznaczonych celów biznesowych jest możliwe nie tylko dzięki posiadaniu typowych składników bilansowych, ale również dzięki składnikowi aktywów, jakim jest właściwe zabezpieczona informacja. Informacja jest zasobem, który trzeba chronić, mając na względzie własne interesy.

Celem artykułu jest przedstawienie roli i znaczenia systemu zarządzania bezpieczeństwem informacji w budowaniu rezyliencji biznesowej współczesnego przedsiębiorstwa. Opracowanie stanowi próbę wskazania najważniejszych kwestii dotyczących ochrony aktywów informacyjnych, które w istotny sposób decydują o rezyliencji biznesowej przedsiębiorstwa. Artykuł składa się z trzech rozdziałów. W pierwszym scharakteryzowano pojęcie i istotę bezpieczeństwa informacji. Drugi prezentuje systemowe zarządzanie bezpieczeństwem informacji. W trzecim przedstawiono zagadnienia związane z kształtowaniem rezyliencji biznesowej przedsiębiorstwa w wyniku implementacji systemu zarządzania bezpieczeństwa informacji. Artykuł powstał na podstawie literatury przedmiotu i wpisuje się w obszar zainteresowań praktyki gospodarczej oraz nauk o zarządzaniu i jakości.

Bezpieczeństwo informacji

Problematyka bezpieczeństwa informacji jest aktualnie przedmiotem zainteresowania wielu przedsiębiorstw. Złożoność środowiska informacyjnego, jak również zakłócenia związane z przepływem informacji uzasadniają potrzebę inwestycji w system bezpieczeństwa informacji.

Przedstawiciel międzynarodowej organizacji DNV, zrzeszającej ekspertów w dziedzinie zapewniania jakości i zarządzania ryzykiem, wskazuje, że najnowsze osiągnięcia technologiczne stały się niezbędnym narzędziem dla wszystkich

[2] A. Chodyński, *Bezpieczeństwo biznesu. Aspekty zarządcze. Wprowadzenie*, „Bezpieczeństwo. Teoria i Praktyka" 2023, nr 4, s. 7–10.

organizacji. Zarówno procesy wykorzystywane obecnie przez firmy, jak i informacje, którymi się posługują, przeniosły się z nośnika fizycznego na nośnik elektroniczny, innymi słowy – z formatu papierowego na cyfrowy. Transformacja ta oznacza łatwiejszą dostępność, wykorzystanie i obsługę tych informacji, które można przeglądać lub przetwarzać z dowolnego urządzenia cyfrowego (telefonu komórkowego, tabletu, laptopa itp.) za pośrednictwem Internetu. W tym kontekście bezpieczeństwo informacji i ochrona danych stanowią aktualny problem nie tylko dla międzynarodowych korporacji, ale także dla MŚP[3].

Bezpieczeństwo informacji to ochrona informacji przed zagrożeniami w celu zapewnienia ciągłości biznesu, minimalizowania ryzyka biznesowego i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych[4].

Wiele regulacji definiuje bezpieczeństwo informacji jako „ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem". Innymi słowy: musimy chronić nasze dane i systemy przed osobami, które chcą ich nadużywać, celowo lub nieumyślnie, a także przed osobami nieuprawnionymi[5].

Bezpieczeństwo informacji to element składowy całościowego bezpieczeństwa organizacji, czyli bezpieczeństwa fizycznego, osobowo-organizacyjnego, prawnego i informatycznego. Pojęcie to obejmuje zarówno bezpieczeństwo informacji przetwarzanych w systemach teleinformatycznych, jak i bezpieczeństwo informacji występujących poza systemami, w postaci dokumentów papierowych, mikrofilmów, w postaci zapamiętanej i wymienianej przez człowieka bezpośrednio lub za pomocą środków łączności[6].

Przez bezpieczeństwo informacji rozumiemy ochronę przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania przedsiębiorstwa, minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych. Innymi słowy bezpieczeństwo informacji zapewnia odpowiedni poziom poufności, dostępności i integralności danych[7].

Bezpieczeństwo informacji obejmuje wszystkie dane gromadzone oraz przetwarzane w organizacji. Zatem obejmuje ono zarówno nowoczesne systemy

---

3 *Bezpieczeństwo informacji w biznesie: od prostego do złożonego*, DNV, 14.06.2023, https://www.dnv.pl/news/bezpieczenstwo-informacji-w-biznesie-od-prostego-do-zlozonego--244524 [dostęp: 30.11.2024].

4 *Bezpieczeństwo informacji w biznesie*, Polski Instytut Kontroli Wewnętrznej, 2022, https://www.pikw.pl/bezpieczenstwo-informacji,art_257.html [dostęp: 1.12.2024].

5 J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, tłum. G. Kowalczyk, Helion, Gliwice 2022, s. 18.

6 A. Januszko-Szakiel, *Zarządzanie bezpieczeństwem informacji w sektorze MŚP – diagnoza i rekomendacje*, [w:] *Diagnostyka w zarządzaniu informacją: perspektywa informatologiczna*, red. R. Sapa, Biblioteka Jagiellońska, Kraków 2017, s. 394.

7 E. Pietras, *Zagadnienia zarządzania bezpieczeństwem informacji w organizacji*, „Zarządzanie Przedsiębiorstwem" 2016, t. 19, nr 1, s. 22–28.

teleinformatyczne, jak i dane generowane w tradycyjny sposób, np. odręczne notatki. Bezpieczeństwo informacji powinno zagwarantować, że dane będące w posiadaniu organizacji nie zostaną przetworzone w nieuprawniony sposób ani udostępnione nieuprawnionym do tego osobom lub podmiotom. Każda informacja generowana w organizacji powinna podlegać ochronie. Oczywiście poziom zastosowanych zabezpieczeń zależy od istoty i znaczenia danej informacji dla organizacji[8].

W literaturze przedmiotu wielu autorów wskazuje model trzech podstawowych atrybutów bezpieczeństwa informacji, powszechnie określany jako triada PID (Poufność, Integralność i Dostępność) lub triada CIA (*Confidentiality, Integrity and Availability*). To model znakomicie ułatwiający myślenie i dyskutowanie o koncepcjach bezpieczeństwa. Bywa również nazywany triadą CAI (*Confidentiality, Availability and Integrity*) lub – w formie negatywnej – triadą DAD (*Disclosure, Alternation and Denial* – ujawnienie, zmiana i odmowa)[9].

Poza triadą w opracowaniach występują bardziej rozbudowane modele. W tabeli 1 zaprezentowano model oparty na siedmiu atrybutach bezpieczeństwa informacji.

Tabela 1. Atrybuty bezpieczeństwa informacji

Atrybut	Deskrypcja
Poufność	Zapewnienie, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
Integralność	Właściwość polegająca na zapewnieniu dokładności i kompletności.
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
Autentyczność	Zapewnienie, że tożsamość podmiotu lub zasobu jest taka jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji).
Rozliczalność	Zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
Niezawodność	Zapewnienie spójności oraz zamierzonych zachowań i skutków.
Niezaprzeczalność	Brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

Źródło: opracowanie na podstawie J. Werner, E. Szczepaniuk, *Bezpieczeństwo informacyjne organizacji,* „Zeszyty Naukowe AON" 2016, nr 4 (105) s. 169; Dzwonkowski P., *Wymogi norm ISO seria 27000*, https://mf-arch2.mf.gov.pl/c/document_library/get_file?uuid=e3607969-79d0-46c5-8e82-85e27331d5a3&groupId=764034 [dostęp: 1.12.2024].

W aspekcie bezpieczeństwa informacji wskazać należy dwa zasadnicze problemy: wielopostaciowość informacji oraz cykl życia informacji[10]. Zarządzający

[8] C. Szydłowski, *Bezpieczeństwo informacji w logistyce*, „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2015, nr 5 (1), s. 21–40.

[9] J. Andress, *op. cit.*, s. 20–21.

[10] M. Pałęga, *Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych*, „Systemy Wspomagania w Inżynierii Produkcji" 2017, t. 6, nr 9: *Zapewnienie prawidłowości przebiegu i bezpieczeństwa procesów produkcyjnych*, s. 58

przedsiębiorstwem powinni uwzględniać obie kwestie w ramach procesu zarządzania bezpieczeństwem informacji.

Informacja występuje w formie papierowej, ustnej i elektronicznej. W związku z tym przedsiębiorstwo w zależności od przybranej formy zasobu informacyjnego powinno w optymalny sposób zarządzać jego bezpieczeństwem. Niewłaściwe zabezpieczona informacja może być źródłem niepowetowanych strat. Realizacja straty finansowej w aspekcie bezpieczeństwa informacji to często powtarzające się negatywne zdarzenie gospodarcze. W wyniku spadku zaufania ze strony interesariuszy przedsiębiorstwo odnotowuje w dłuższym okresie zmniejszoną sprzedaż towarów bądź usług.

Równie istotnym czynnikiem wpływającym na bezpieczeństwo informacji jest cykl życia informacji. Informacja powstaje, następnie można ją przekazać, przetworzyć (zmodyfikować), kopiować. Informację można wykorzystać, przechowywać, gromadzić. Można ją również utracić albo zniszczyć. Kwestią dyskusyjną pozostaje możliwość uszkodzenia informacji. Nośnik przechowujący informację może zostać zniszczony, przez co informacja zawarta na tym nośniku ulega zniszczeniu[11]. Można zauważyć, że występuje tu wiele newralgicznych momentów, podczas których może wystąpić naruszenie bezpieczeństwa informacji. Wobec tego w każdym przedsiębiorstwie istnieje uzasadniona potrzeba wdrożenia systemu zarządzania bezpieczeństwem informacji, który zapewni przedsiębiorstwu rezyliencję.

Wymagania prawne dotyczące bezpieczeństwa informacyjnego są kolejną kwestią, którą należy uwzględnić. Określenie bezpieczeństwa informacji w przedsiębiorstwie będzie zależało w szczególności od ram prawnych, na podstawie których i w ramach których funkcjonuje dany podmiot gospodarczy. Przedsiębiorstwa nie zdają sobie zazwyczaj sprawy z mnogości aktów normatywnych w tej dziedzinie. W związku z istnieniem szerokiego wachlarza aktów normatywnych w zakresie bezpieczeństwa informacji można dokonać ich podziału w następujący sposób[12]:

- normy słownikowe (dostarczające podstawowe definicje dotyczące systemów zarządzania bezpieczeństwem informacji),
- normy zawierające wymagania (wskazujące zalecenia dla prowadzących audyt i certyfikację systemów),
- normy zawierające wytyczne (przedstawiające praktyczne zasady zarządzania ryzykiem i bezpieczeństwem informacji),
- normy zawierające wytyczne dla specyficznych, określonych sektorów (określające rozwiązania branżowe),
- normy zawierające specyficzne zabezpieczenia (prezentujące narzędzia i techniki profilaktyki bezpieczeństwa).

---

[11] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010, s. 11.

[12] K. Bobkowski, *Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji*, „Zarządzanie i Finanse" 2018, t. 16, nr 3, cz. 2, s. 20–23.

Systemowe zarządzanie bezpieczeństwem informacji

Bezpieczeństwo informacji jest realizowane poprzez wdrażanie odpowiedniego systemu zabezpieczeń, w tym polityki, procesów, procedur, struktury organizacyjnej, funkcji oprogramowania i sprzętu. Zabezpieczenia te muszą zostać ustanowione, wdrożone, monitorowane, sprawdzone i udoskonalone (w razie potrzeby), w celu zapewnienia, że wymagania bezpieczeństwa i realizacji celów biznesowych organizacji są spełnione. Uzyskanie i utrzymanie właściwego poziomu bezpieczeństwa każdej działalności wymaga szeregu przedsięwzięć znacznie wykraczających poza potocznie uświadamiane potrzeby w tym zakresie. Niezależnie od formy informacji oraz sposobów, za pomocą których jest ona przetwarzana, przesyłana lub przechowywana, powinna być zawsze odpowiednio zabezpieczona[13].

W ostatnich latach obserwujemy znaczący wzrost zainteresowania przedsiębiorstw wdrożeniem systemu zarządzania bezpieczeństwem informacji. Główne przyczyny tej popularności można podzielić na trzy grupy, które są związane[14]:

- ze wzrostem znaczenia informacji w gospodarce,
- z pogłębianiem współpracy pomiędzy przedsiębiorstwami,
- z rosnącym poziomem trudności zarządzania informacjami.

Najistotniejsze wydają się zagrożenia informacyjne, których występowanie stanowi bardzo duże wyzwanie dla przedsiębiorstw. Dzięki systemowemu podejściu do zarządzania bezpieczeństwem informacji, opartemu na efektywnie przeprowadzonej ocenie ryzyka, można w przedsiębiorstwie zapewnić skuteczne mitygowanie zagrożeń. Przykładami najczęściej występujących zagrożeń informacji są[15]:

- brak informacji,
- chaos informacyjny,
- cyberterroryzm,
- działalność grup świadomie manipulujących przekazem,
- przestępstwa komputerowe,
- walka informacyjna,
- szpiegostwo,
- niekontrolowany rozwój nowych technologii,
- nieprawidłowe ujawnienie informacji,
- asymetria w wymianie informacji,
- naruszenie przez władzę praw obywatelskich.

---

13 *Bezpieczeństwo informacji w biznesie*, PIKW, *op. cit*.

14 S. Wawak, *Podejście procesowe we wdrażaniu systemów zarządzania bezpieczeństwem informacji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2009, nr 52: *Podejście procesowe w organizacjach*, s. 127.

15 D. Rydz, M. Krakowiak, T. Bajor, *Zapewnienie bezpieczeństwa informacji w przedsiębiorstwach*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa" 2013, t. 1, s. 285.

Ostatnia edycja raportu *Allianz Risk Barometer 2024*, która opiera się na wynikach ankiety przeprowadzonej wśród 3069 respondentów z 92 krajów, obejmującej brokerów ubezpieczeniowych, konsultantów ds. ryzyka i innych ekspertów, wskazuje 10 najważniejszych zagrożeń, z którymi przedsiębiorstwa będą musiały się zmierzyć. Cyberincydenty okazały się największym globalnym ryzykiem, z wyraźną przewagą nad pozostałymi (36% odpowiedzi, 5 punktów procentowych przewagi nad drugim w kolejności ryzykiem przerw w działalności (*Business Interruption*, BI))[16].

Zarządzanie bezpieczeństwem informacji jest procesem bardzo złożonym, gdyż w zależności od profilu działalności organizacji informacje będą zróżnicowane pod względem istotności, wartości i przydatności. Wpisanie konieczności zapewnienia bezpieczeństwa informacyjnego do strategii organizacji odgrywa istotną rolę w pomyślnej realizacji jego celów. Zapewnienie bezpieczeństwa informacji staje się warunkiem koniecznym, wpisującym się w zakresy obowiązków kadry zarządzającej. Wyzwania stojące przed najwyższym kierownictwem związane z wdrożeniem odpowiedniego modelu bezpieczeństwa informacji w celu utrzymania ładu organizacyjnego stają się niejednokrotnie zadaniem przerastającym organizację. W związku z powyższym konieczne jest wdrożenie sprawdzonych standardów zarówno w aspekcie technicznym, jak i organizacyjnym[17]. Organizacja, która chce należycie zabezpieczyć swoje informacje, powinna zastosować podejście systemowe, w ramach którego będzie kompleksowo zarządzać posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji.

Jednym z rozwiązań jest standard System Zarządzania Bezpieczeństwem Informacji (SZBI, ang. *Information Security Management System*, ISMS), zgodny z ISO/IEC 27001 o międzynarodowym zasięgu. System ten określa wymagania, zasady inicjowania, wdrażania, utrzymania i poprawy zarządzania bezpieczeństwem informacji w organizacji oraz zawiera cele i praktyki stosowanych zabezpieczeń w następujących obszarach zarządzania bezpieczeństwem informacji[18]:

- polityka bezpieczeństwa informacji,
- organizacja bezpieczeństwa informacji,
- bezpieczeństwo zasobów ludzkich,
- zarządzanie aktywami,
- kontrola dostępu,
- kryptografia,
- bezpieczeństwo fizyczne i środowiskowe,

---

16 *Allianz Risk Barometer 2024*, Allianz, https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html#download [dostęp: 30.11.2024].

17 K. Bobkowski, *op. cit.*, s. 17–30.

18 *Wdrożenie ISO 27001 – System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami ISO 27001*, Malon Group, https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/iso-27001 [dostęp: 1.12.2024].

- bezpieczeństwo komunikacji,
- pozyskiwanie, rozwój i utrzymanie systemów,
- relacje z dostawcami,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania,
- zgodność.

Organizacja, aby wprowadzić skuteczny system bezpieczeństwa informacji, powinna[19]:

- wdrożyć system aktualizacji obowiązujących w organizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia oraz pojawiających się zagrożeń dla bezpieczeństwa informacji przetwarzanych w przedsiębiorstwie,
- monitorować stan posiadanego sprzętu oraz oprogramowania wykorzystywanego do przetwarzania informacji w przedsiębiorstwie,
- prowadzić okresowy przegląd oraz analizę potencjalnych zagrożeń (ryzyk) w zakresie bezpieczeństwa informacji oraz systemów teleinformatycznych w przedsiębiorstwie,
- dążyć do doskonalenia umiejętności oraz kompetencji pracowników zaangażowanych w proces przetwarzania informacji, w celu zapewnienia posiadania przez nich aktualnych uprawnień umożliwiających im skuteczną realizację zadań w zakresie zapewnienia bezpieczeństwa informacji,
- przeprowadzać okresowe szkolenia pracowników przetwarzających dane, ze szczególnym uwzględnieniem problematyki zagrożenia bezpieczeństwa informacji oraz skutków naruszenia zasad bezpieczeństwa informacji, w celu minimalizacji potencjalnych zagrożeń dla bezpieczeństwa danych, wprowadzać systemy ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- wdrożyć skuteczne systemy dostępu do informacji przetwarzanych w firmie,
- wdrożyć procedury prowadzące do ustalenia przyczyn oraz osób odpowiedzialnych za wystąpienie przypadków naruszenia bezpieczeństwa informacji,
- wdrożyć skuteczne środki uniemożliwiające nieautoryzowany dostęp do systemów operacyjnych, usług sieciowych oraz aplikacji wykorzystywanych w firmie,
- wdrożyć procedury oraz mechanizmy zapewniające bezpieczną pracę przy mobilnym przetwarzaniu informacji przez pracowników oraz przy pracy zdalnej,
- wdrożyć procedury oraz mechanizmy zabezpieczające informacje przed nieuprawnionym ujawnieniem, modyfikacjami, usunięciem lub zniszczeniem,
- zawrzeć w umowach serwisowych z usługodawcami zapisy gwarantujące organizacji odpowiedni poziom bezpieczeństwa informacji,

[19] C. Szydłowski, *op. cit*.

- wdrożyć procedury oraz mechanizmy zapewniające bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących,
- wdrożyć obowiązek okresowego przeprowadzania audytu bezpieczeństwa informacji oraz systemów teleinformatycznych wykorzystywanych przez przedsiębiorstwo,
- wdrożyć procedury oraz mechanizmy minimalizacji ryzyka kradzieży informacji i urządzeń teleinformatycznych, w tym urządzeń mobilnych,
- wdrożyć procedury oraz mechanizmy zapewniające firmie odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych.

ISMS ma zapewnić odpowiedni poziom rezyliencji przedsiębiorstwa na zakłócenia i zagrożenia związane z bezpieczeństwem informacji, które mogłyby wywrzeć negatywny wpływ na ciągłość działania przedsiębiorstwa oraz na realizację przyjętych celów biznesowych. Na rysunku 1 zilustrowano korzyści z wdrożenia systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie.

Rysunek 1. Korzyści z implementacji ISMS

Źródło: opracowanie na podstawie *The Key Benefits of ISO/IEC 27001 Certification Explained*, Sprintzeal, 27.06.2024, https://www.sprintzeal.com/blog/benefits-of-iso-27001-certification [dostęp: 5.12.2024]; *Strengthening information security: How ISO 27001 enables compliance and cyber resilience*, BDO Canada, 10.09.2024, https://www.bdo.ca/insights/strengthening-information-security-how-iso-27001-enables-compliance-and-cyber-resilience [dostęp: 5.12.2024].

Bardzo ważnym elementem systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie jest kultura bezpieczeństwa. Praktyka utrzymania bezpieczeństwa na odpowiednim poziomie wymaga stosowania właściwych rozwiązań technicznych chroniących przed zagrożeniami po stronie klienta/użytkownika oraz realizowania programu *Security Awareness* (świadomość bezpieczeństwa) w celu permanentnego budowania kultury bezpieczeństwa wśród wszystkich użytkowników sieci wewnętrznej. W realiach organizacji są to pewne wzorce zachowań, przekonania, postawy i sposoby działania, które składają się na kulturę tejże organizacji. Kultura bezpieczeństwa informacji powinna stanowić ważną część kultury organizacji. Docelowo powinna być dobrze zorganizowana, spójna i skuteczna – tak aby mogła wspierać w działaniu osoby, które uznają, że bezpieczeństwo jest jednym ze strategicznych atrybutów funkcjonowania organizacji[20].

Ocena poziomu kultury bezpieczeństwa informacyjnego zarówno jednostki, jak i zbiorowości stanowi punkt wyjścia do tworzenia polityki bezpieczeństwa informacyjnego organizacji. Stąd w ramach ewaluacji procesu bezpieczeństwa informacyjnego jednym z elementów poddawanych ocenie jest kultura informacyjna pracowników, stanowiąca element kultury organizacyjnej audytowanej instytucji[21]. Rozwijanie kultury bezpieczeństwa informacji sprzyja budowaniu rezyliencji przedsiębiorstwa.

Rezyliencja biznesowa przedsiębiorstwa jako rezultat wdrożenia systemu zarządzania bezpieczeństwem informacji

Budowanie rezyliencji biznesowej jest niezmiernie ważne dla współczesnych przedsiębiorstw. Zarządzający przedsiębiorstwami powinni zdawać sobie sprawę, że aby realizować cele biznesowe w świecie VUCA, wymaga się od nich kompetencji w zakresie osiągania rezyliencji biznesowej. W takiej rzeczywistości – zmiennej, niepewnej, złożonej i niejednoznacznej – menedżerowie i projektanci napotykają nowe bariery i trudności pojawiające się w procesach rozwiązywania problemów organizacyjnych, w tym problemów bezpieczeństwa, gdyż niektóre z nich nie dają się rozwiązać nawet przy użyciu najbardziej wyrafinowanych narzędzi analitycznych[22].

Kiedy mówimy o rezyliencji w naukach społecznych, uwzględniamy badanie odporności w systemach środowiskowych, gospodarczych i politycznych. Rezyliencja to

[20] W. Józefowicz, *Kształtowanie kultury bezpieczeństwa informacji*, „Wiedza Obronna" 2016, nr 1–2, s. 144–145.

[21] H. Batorowska, *Obszary kultury bezpieczeństwa informacyjnego i jej badanie*, „Kultura Bezpieczeństwa" 2018, nr 10, s. 13–33, https://czasopisma.uph.edu.pl/kulturabezpieczenstwa/article/view/1826 [dostęp: 4.12.2024].

[22] J. Ziarko, *Uwarunkowania zarządzania problemami bezpieczeństwa w świecie VUCA*, „Bezpieczeństwo. Teoria i Praktyka" 2024, nr 1, s. 23, https://doi.org/10.48269/2451-0718-btip-2024-1-001.

zdolność do adaptacji istniejących zasobów i umiejętności do nowych sytuacji i warunków działania[23]. Na poziomie organizacyjnym odporność jest rozumiana jako zdolność przedsiębiorstwa do przetrwania w obliczu istotnych zmian w otoczeniu biznesowym i gospodarczym i/lub zdolność przeciwstawienia się zakłóceniom i katastroficznym wydarzeniom[24]. Rezyliencja organizacji to mierzalna kombinacja cech, zdolności lub możliwości, która pozwala organizacji przeciwstawić się znanym i nieznanym zakłóceniom – i przetrwać[25]. Rezyliencja organizacji to zdolność do absorpcji i adaptacji w zmieniającym się środowisku. To kategoria wielowymiarowa, na którą wpływa wiele czynników strategicznych i operacyjnych.

Rezyliencja operacyjna jest wynikiem działań łagodzących podejmowanych przez system zarządzania ryzykiem przedsiębiorstwa. Chociaż rezyliencja operacyjna tradycyjnie jest zarządzana za pośrednictwem ram ryzyka operacyjnego, wiele ryzyk kształtujących jej poziom ma charakter finansowy. Skutki finansowe mają tendencję do bycia nagłymi i wysoce dotkliwymi. Należy je zmierzyć, aby lepiej zrozumieć ich istotę oraz aby działania łagodzące były skuteczne[26].

Cyberrezyliencja to koncepcja łącząca ciągłość biznesową, bezpieczeństwo systemów informatycznych i rezyliencję organizacji. Koncepcja ta opisuje zdolność do ciągłego dostarczania zamierzonych rezultatów pomimo doświadczania trudnych zdarzeń cybernetycznych, takich jak cyberataki. Zmierzony poziom biegłości w zakresie bezpieczeństwa informacji i odporności wpływa na to, jak dobrze organizacja może kontynuować działalność biznesową z niewielkim lub żadnym przestojem[27].

Z kolei rezyliencja biznesowa to zdolność organizacji do szybkiego przystosowania się do nieoczekiwanych sytuacji zakłóceń – i zapobiegania zatrzymaniu wszelkich bieżących przepływów pracy, przy jednoczesnym utrzymaniu ciągłości działalności operacji i zabezpieczania ludzi, zasobów, majątku i kapitału własnego[28]. Rezyliencja biznesowa to stan, w którym właściciele firm (lub firmy) mają zdolność lepszego zarządzania potencjalnymi kryzysami, które mogą wystąpić, i stawienia czoła przyszłym

---

[23] S.C. Smith, *Toward a Scientific Definition of Cyber Resilience*, DEVCOM Army Research Laboratory, ARL-TR-9716, 2023.

[24] M. Morisse, C. Prigge, *Design of a business resilience model for Industry 4.0 manufacturers*, Twenty-third Americas Conference on Information Systems, Boston 2017, s. 1–10.

[25] S. Vargas, H.A. Rivera, *Business resilience: a dynamic capability to overcome extreme adversity*, „Revista Espacios" 2019, t. 40, nr 6, https://revistaespacios.com/a19v40n06/a19v40n06p05.pdf [dostęp: 5.12.2024].

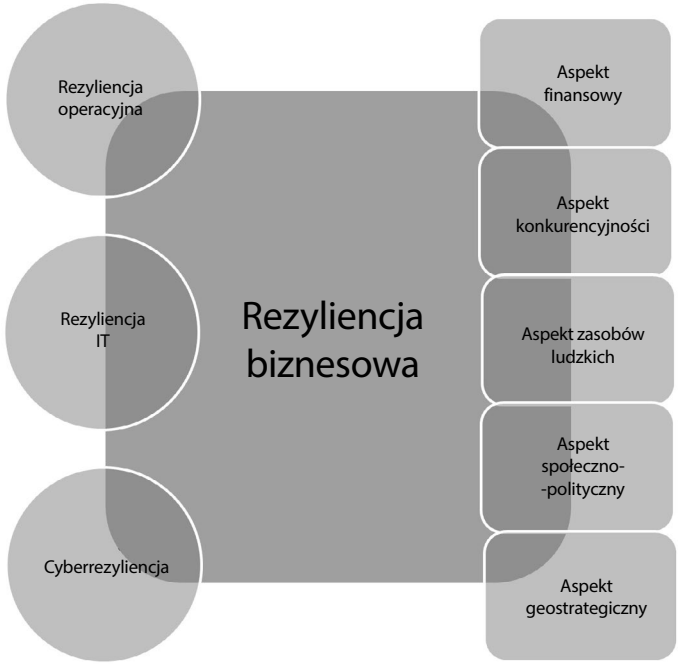
[26] R.D. Chanon *et al.*, *Operational Resilience in the UK Financial Sector*, Institute and Faculty of Actuaries, 12.08.2024, s. 15, https://vle.actuaries.org.uk/pluginfile.php/152254/mod_resource/content/2/RM%20Operational%20Resilience%20in%20the%20UK%20Financial%20Sector%20TFG%20Paper%2012082024.pdf [dostęp: 15.12.2024].

[27] *What is cyber resilience?*, IBM, 20.01.2022, https://www.ibm.com/topics/cyber-resilience [dostęp: 29.11.2024].

[28] B. Zohuri, M. Moghaddam, F. Mossavar-Rahmani, *Business resilience system integrated artificial intelligence system*, „International Journal of Theoretical & Computational Physics" 2022, t. 3, s. 1–7.

wyzwaniom[29]. Rezyliencja biznesowa oznacza, że przedsiębiorstwo wykazuje zdolność do odnowienia krytycznych funkcji, zasobów. Ponadto obejmuje wszystkie aspekty organizacji, takie jak zasoby ludzkie, procesy biznesowe, infrastruktura[30]. Rezyliencja biznesowa przedsiębiorstwa ma charakter wielowymiarowy i nie można jej osiągnąć, zajmując się tylko jednym, wybranym aspektem działalności. Dzięki rezyliencji biznesowej przedsiębiorstwo ma znacznie większą kontrolę nad rezyliencją operacyjną, rezyliencją IT i cyberrezyliencją. Te rodzaje rezyliencji dotyczą głównie nieprzewidzianych, zakłócających zdarzeń, które mają miejsce w horyzoncie krótkoterminowym lub natychmiastowym firmy[31]. Na rysunku 2 przedstawiono aspekty wielowymiarowości rezyliencji biznesowej.

Rysunek 2. Wielowymiarowość rezyliencji biznesowej



Źródło: opracowanie na podstawie *Business Resilience A-to-Zerto Glossary of Terms*, Zerto, https://www.zerto.com/resources/a-to-zerto/business-resilience [dostęp: 5.12.2024].

[29] A.D. Prawestri, W.D. Silviani, Y. Astuti, *The role of financial knowledge and behaviour to sustain future business resilience*, „Annual International Conference on Islamic Economics and Business (AICIEB)" 2022, t. 2, nr 1, s. 212–223.

[30] M. Soliwoda, *Odporność z perspektywy ekonomii i finansów. Wybrane problemy*, Instytut Ekonomiki Rolnictwa i Gospodarki Żywnościowej – Państwowy Instytut Badawczy, Warszawa 2020, s. 39.

[31] *Business Resilience A-to-Zerto Glossary of Terms*, Zerto, https://www.zerto.com/resources/a-to-zerto/business-resilience [dostęp: 5.12.2024].

Rezyliencja biznesowa to system odpornościowy zbudowany na kombinacji wymiaru strategicznego, finansowego, operacyjnego, informatycznego i ludzkiego. Przedsiębiorstwo, uzyskując przewagę konkurencyjną w zakresie bezpieczeństwa informacji, wzmacnia swoją reputację. Osiągnięcie przez przedsiębiorstwo dojrzałości pod względem rezyliencji biznesowej zapewnia ochronę przed absorbowaniem zdarzeń zakłócających. Dzięki temu kadra zarządzająca skupiona jest na realizacji celów biznesowych oraz rozwoju przedsiębiorstwa.

Przedstawiciele Boston Consulting Group (BCG), międzynarodowej amerykańskiej firmy będącej liderem w zakresie doradztwa strategicznego, przypominają, że każda organizacja musi polegać na danych, analizach i technologiach cyfrowych. Podkreślają, że automatyzacja i technologie cyfrowe będą stanowić coraz bardziej krytyczny element rezyliencji biznesowej. Ponadto zwracają uwagą na fakt, że inwestycje w rozwiązania cyfrowe zapewnią przedsiębiorstwu odporność, przyspieszą szybkie wychodzenie z kryzysów oraz umożliwią tworzenie zrównoważonej przewagi konkurencyjnej. BCG przeprowadziło w 2019 r. badanie wśród przedsiębiorstw, którego wynik pokazuje, że dzięki transformacji cyfrowej przedsiębiorstwa budują długoterminową rezyliencję poprzez[32]:

- zwiększenie szybkości wprowadzenia produktów/usług na rynek (od 40% do 50%),
- zwiększenie wydajności pracowników (od 20% do 30%),
- zwiększenie stabilności systemów informatycznych (do 60%),
- zwiększenie wyniku operacyjnego (od 12% do 20%).

Zatem wdrożenie systemu bezpieczeństwa informacji jest właściwym rozwiązaniem w kierunku budowania odporności biznesowej przedsiębiorstwa. Z punktu widzenia przedsiębiorstwa inwestycja w nowoczesne rozwiązania cyfrowe jest jak najbardziej uzasadniona biznesowo.

Podsumowanie

Obecny stopień informatyzacji i perspektywa jego rozwoju przyczynia się do zwiększenia ilości przetwarzanych informacji przez przedsiębiorstwa, a tym samym do większego wolumenu potencjalnych negatywnych oddziaływań na dostępność i integralność informacji. Istnieje zatem potrzeba pilnego zapewnienia bezpieczeństwa informacji, w szczególności stosowania odpowiedniego do ryzyka poziomu ochrony aktywów informacyjnych.

Przedsiębiorstwo poprzez wdrożenie systemu zarządzania bezpieczeństwem informacji staje się dysponentem instrumentu, który eliminuje lub redukuje ryzyko

[32] K. Close *et al.*, *The Digital Path to Business Resilience*, Boston Consulting Group, 6.07.2020, https://www.bcg.com/publications/2020/digital-path-to-business-resilience [dostęp: 5.12.2024].

wystąpienia zdarzeń związanych z bezpieczeństwem informacji. Można zauważyć, że implementacja systemowych narzędzi i mechanizmów w odniesieniu do regulacji wynikających z przepisów prawa w zakresie bezpieczeństwa informacji gwarantuje odpowiedni poziom rezyliencji biznesowej. Przedsiębiorstwo uzyskuje odporność na zakłócenia w przypadku materializacji zagrożeń. Odwołując się do literatury przedmiotu, należy stwierdzić, że tematyka rezyliencji biznesowej i systemowego zarządzania bezpieczeństwem informacji jest niezmiernie ważna dla dzisiejszego świata biznesu.

Bibliografia

Allianz Risk Barometer 2024, Allianz, https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html#download [dostęp: 30.11.2024].

Andress J., *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, tłum. G. Kowalczyk, Helion, Gliwice 2022.

Batorowska H., *Obszary kultury bezpieczeństwa informacyjnego i jej badanie*, „Kultura Bezpieczeństwa" 2018, nr 10, s. 13–33, https://czasopisma.uph.edu.pl/kulturabezpieczenstwa/article/view/1826 [dostęp: 4.12.2024].

Bezpieczeństwo informacji w biznesie, Polski Instytut Kontroli Wewnętrznej, 2022, https://www.pikw.pl/bezpieczenstwo-informacji,art_257.html [dostęp: 1.12.2024].

Bezpieczeństwo informacji w biznesie: od prostego do złożonego, DNV, 14.06.2023, https://www.dnv.pl/news/bezpieczenstwo-informacji-w-biznesie-od-prostego-do-zlozonego--244524 [dostęp: 30.11.2024].

Bobkowski K., *Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji*, „Zarządzanie i Finanse" 2018, t. 16, nr 3, cz. 2, s. 17–30.

Business Resilience A-to-Zerto Glossary of Terms, Zerto, https://www.zerto.com/resources/a-to-zerto/business-resilience [dostęp: 5.12.2024].

Chanon R.D., Habahbeh L., Klumpes P., Mann S., *Operational Resilience in the UK Financial Sector*, Institute and Faculty of Actuaries, 12.08.2024, s. 15, https://vle.actuaries.org.uk/pluginfile.php/152254/mod_resource/content/2/RM%20Operational%20Resilience%20in%20the%20UK%20Financial%20Sector%20TFG%20Paper%2012082024.pdf [dostęp: 15.12.2024].

Close K., Grebe M., Andersen P., Khurana V., Franke M.R., Kalthof R., *The Digital Path to Business Resilience*, Boston Consulting Group, 6.07.2020, https://www.bcg.com/publications/2020/digital-path-to-business-resilience [dostęp: 5.12.2024].

Chodyński A., *Bezpieczeństwo biznesu. Aspekty zarządcze. Wprowadzenie*, „Bezpieczeństwo. Teoria i Praktyka" 2023 , nr 4, s. 7–10.

Dzwonkowski P., *Wymogi norm ISO seria 27000*, https://mf-arch2.mf.gov.pl/c/document_library/get_file?uuid=e3607969-79d0-46c5-8e82-85e27331d5a3&groupId=764034 [dostęp: 1.12.2024].

Fleszer D., *Wokół problematyki bezpieczeństwa informacji*, „Rocznik Administracji i Prawa" 2018, t. 1, nr XVIII, s. 187–199, https://doi.org/10.5604/01.3001.0012.5998.

Januszko-Szakiel A., *Zarządzanie bezpieczeństwem informacji w sektorze MŚP – diagnoza i rekomendacje*, [w:] *Diagnostyka w zarządzaniu informacją: perspektywa informatologiczna*, red. R. Sapa, Biblioteka Jagiellońska, Kraków 2017, s. 391–413.

Józefowicz W., *Kształtowanie kultury bezpieczeństwa informacji*, „Wiedza Obronna" 2016, nr 1–2, s. 140–151.

The Key Benefits of ISO/IEC 27001 Certification Explained, Sprintzeal, 27.06.2024, https://www.sprintzeal.com/blog/benefits-of-iso-27001-certification [dostęp: 5.12.2024].

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.

Morisse M., Prigge C., *Design of a business resilience model for Industry 4.0 manufacturers*, Twenty-third Americas Conference on Information Systems, Boston 2017, s. 1–10.

Pałęga M., *Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych*, „Systemy Wspomagania w Inżynierii Produkcji" 2017, t. 6, nr 9: *Zapewnienie prawidłowości przebiegu i bezpieczeństwa procesów produkcyjnych*, s. 58–70.

Pietras E., *Zagadnienia zarządzania bezpieczeństwem informacji w organizacji*, „Zarządzanie Przedsiębiorstwem" 2016, t. 19, nr 1, s. 22–28.

Prawestri A.D., Silviani W.D., Astuti Y., *The role of financial knowledge and behaviour to sustain future business resilience*, „Annual International Conference on Islamic Economics and Business (AICIEB)" 2022, t. 2, nr 1, s. 212–223.

Rydz D., Krakowiak M., Bajor T., *Zapewnienie bezpieczeństwa informacji w przedsiębiorstwach*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa" 2013, t. 1, s. 281–287.

Smith S.C., *Toward a Scientific Definition of Cyber Resilience*, DEVCOM Army Research Laboratory, ARL-TR-9716, 2023.

Strengthening information security: How ISO 27001 enables compliance and cyber resilience, BDO Canada, 10.09.2024, https://www.bdo.ca/insights/strengthening-information-security-how-iso-27001-enables-compliance-and-cyber-resilience [dostęp: 5.12.2024].

Szydłowski C., *Bezpieczeństwo informacji w logistyce*, „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2015, nr 5 (1), s. 21–40.

Soliwoda M., *Odporność z perspektywy ekonomii i finansów. Wybrane problemy*, Instytut Ekonomiki Rolnictwa i Gospodarki Żywnościowej – Państwowy Instytut Badawczy, Warszawa 2020.

Vargas S., Rivera H.A., *Business resilience: a dynamic capability to overcome extreme adversity*, „Revista Espacios" 2019, t. 40, nr 6, https://revistaespacios.com/a19v40n06/a19v40n06p05.pdf [dostęp: 5.12.2024].

Wawak S., *Podejście procesowe we wdrażaniu systemów zarządzania bezpieczeństwem informacji*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2009, nr 52: *Podejście procesowe w organizacjach*, s. 127–135.

What is cyber resilience?, IBM, 20.01.2022, https://www.ibm.com/topics/cyber-resilience [dostęp: 29.11.2024].

Wdrożenie ISO 27001 – System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami ISO 27001, Malon Group, https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/iso-27001 [dostęp: 1.12.2024].

Werner J., Szczepaniuk E., *Bezpieczeństwo informacyjne organizacji*, „Zeszyty Naukowe AON" 2016, nr 4 (105), s. 167–187.

Ziarko J., *Uwarunkowania zarządzania problemami bezpieczeństwa w świecie VUCA*, „Bezpieczeństwo. Teoria i Praktyka" 2024, nr 1, s. 23–41.

Zohuri B., Moghaddam M., Mossavar-Rahmani F., *Business resilience system integrated artificial intelligence system*, „International Journal of Theoretical & Computational Physics" 2022, t. 3, s. 1–7.

Rola systemu zarządzania bezpieczeństwem informacji w budowaniu rezyliencji biznesowej przedsiębiorstwa
Streszczenie

W artykule poruszono zagadnienie roli i znaczenia systemu zarządzania bezpieczeństwem informacji w budowaniu rezyliencji biznesowej współczesnego przedsiębiorstwa. Zwrócono uwagę na fakt, że zapewnienie bezpieczeństwa informacji to zadanie każdej organizacji będącej w posiadaniu aktywów informacyjnych. Turbulentne otoczenie przedsiębiorstwa tylko dynamizuje trudności zarządzania informacjami. Kadra zarządzająca mająca świadomość występujących zagrożeń i chcąca chronić przedsiębiorstwo przed negatywnymi konsekwencjami finansowymi powinna kształtować rezyliencję biznesową. Ponadto pokazano, że bardzo ważnym elementem systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie jest kultura bezpieczeństwa. Do prezentacji omawianych zagadnień wykorzystano metodę analizy literatury, a także raportów i opracowań organizacji doradztwa gospodarczego w przedmiotowym obszarze.

Słowa kluczowe: bezpieczeństwo informacji, system zarządzania bezpieczeństwem informacji, rezyliencja, rezyliencja biznesowa

The role of the information security management system in building business resilience of the enterprise
Abstract

The article discusses issues regarding the role and importance of the information security management system in building the business resilience of a modern enterprise. Attention was drawn to the fact that ensuring information security is the task of every organization in possession of information assets. The turbulent environment of the company only increases the difficulties of information management. The top management staff, being aware of the existing threats, should develop business resilience in order to protect the company against negative financial consequences. Moreover, it was shown that security culture is a very important element of the information security management system in an enterprise. To present the discussed issues, the method of literature analysis was used, as well as reports and studies of economic consulting organizations in the subject area.

Keywords: information security, information security management system, resilience, business resilience