University of Economics in Katowice

ARBE ACADEMIC REVIEW OF BUSINESS AND ECONOMICS

ISSN 2720-457X Vol. 2(1) · 2022

Identyfikacja zagrożeń wynikających z użytkowania systemów informatycznych

Adrian Mencel

Uniwersytet Ekonomiczny w Katowicach, Koło Naukowe Analiz Rynku Finansowego, adrian.mencel@edu.uekat.pl, ORCID: 0000-0002-8667-8183

Streszczenie: Prawidłowe sklasyfikowanie zagrożeń, na które są narażone systemy informatyczne użytkowane w przedsiębiorstwach, może zapewnić odpowiedni dobór sposobów ich zabezpieczenia. Stworzenie jednorodnej i spójnej klasyfikacji może pozwolić na porównanie opisanych zagrożeń między różnymi systemami informatycznymi użytkowanymi w przedsiębiorstwach. Celem artykułu jest propozycja klasyfikacji źródeł zagrożeń systemów informatycznych oraz zbadanie, czy polskie przedsiębiorstwa identyfikują zagrożenia tych systemów. Badanie ma charakter pilotażu. Metodą badawczą przyjętą w opracowaniu jest przegląd literatury, badań naukowych oraz analiza sprawozdań zarządu badanych 18 spółek z sektora transportu i logistyki, energetycznego oraz telekomunikacyjnego z indeksu WIG za lata 2019-2020. Na podstawie przeprowadzonych rozważań stwierdzono, iż zaprezentowana klasyfikacja pozwala zidentyfikować zagrożenia systemów informatycznych oraz może pomóc w ich zabezpieczeniu. Przeprowadzona w artykule analiza dowiodła, że spółki z sektora transportu i logistyki, energetycznego i telekomunikacyjnego ujawniają niewiele informacji o występujących w ich działalności zagrożeniach systemów informatycznych, a co z tym związane − sposobach ich zabezpieczenia. Spółki z sektora energetycznego ujawniają znacznie więcej informacji, a spółki z sektora telekomunikacyjnego wykazują najwięcej.

Słowa kluczowe: systemy informatyczne, zagrożenia systemów informatycznych, klasyfikacja źródeł zagrożeń systemów informatycznych.

Kod JEL: M15, M41, K24, L86.

1. Wstęp

Systemy informatyczne mają zastosowanie w wielu obszarach przedsiębiorstwa i generują wiele korzyści dla przedsiębiorstw w takich obszarach, jak: finanse, księgowość, zarządzanie i planowanie poprzez wsparcie procesów tech-

Sposób cytowania: Mencel, A. (2022). Identyfikacja zagrożeń wynikających z użytkowania systemów informatycznych. *Academic Review of Business and Economics, 2*(1), 79-94. https://doi.org/10.22367/arbe.2022.02.05

nologii produkcji czy logistyki dostaw (Król-Stępień, 2013, s. 76). Systemy te przyczyniają się do obniżenia kosztów działalności, a zaawansowane programy informatyczne pozwalają wykonywać większość operacji automatycznie. Wpływa to na skrócenie czasu potrzebnego na realizację określonych czynności, zwłaszcza w procesach sprzedaży, finansowych czy logistycznych, np. realizacja zamówień, księgowanie operacji gospodarczych, zarządzanie magazynem.

Bezpieczeństwo informacji od zawsze było priorytetem dla przedsiębiorstw, szczególnie w odniesieniu do danych strategicznych dla ich działalności, tzw. know-how, do którego zalicza się m.in. metody produkcji danego dobra, wypracowane schematy w sposobach komunikacji wewnątrz jednostki czy metody rozwiązywania konfliktów wewnątrz jednostki. W dobie transformacji cyfrowej prawidłowe zabezpieczenie danych i informacji stało się kluczowe. Ilość przetwarzanych przez przedsiębiorstwa informacji stale wzrasta, a wraz z nią liczba i złożoność zagrożeń. Im więcej zasobów do ochrony, tym więcej możliwości do nadużyć (Kunz & Tymińska, 2014, s. 47).

Szczególnym priorytetem powinna być ochrona zasobów informacji przedsiębiorstw strategicznych, czyli m.in. dostawców energii elektrycznej i surowców energetycznych, firm odpowiadających za utrzymanie sieci telekomunikacyjnej, przedsiębiorstw prowadzących linie lotnicze, kolejowe czy metro. Narażony na zagrożenia systemów informatycznych jest również sektor transportu i logistyki. Niezapewnienie bezpieczeństwa dla systemów informatyczno-logistycznych może skutkować przerwami w dostawach dla pozostałych sektorów gospodarki państwa.

Wskazane przykłady determinują konieczność sporządzenia odpowiedniej klasyfikacji źródeł zagrożeń systemów informatycznych, która ułatwi przedsiębiorstwom przejmowanie i odpowiedni dobór rozwiązań w zakresie zabezpieczeń z innych systemów informatycznych. Zanim jednostki podejmą decyzję o sporządzeniu klasyfikacji możliwych źródeł zagrożeń informatycznych i nadadzą im odpowiednią rangę, powinny dokonać przeglądu możliwych do wystąpienia zagrożeń dla ich działalności gospodarczej. Dlatego też dopełnieniem zaproponowanej w artykule klasyfikacji będzie przeprowadzone badanie pod kątem sprawdzenia, czy jednostki z sektora transportu i logistyki, energetyki i telekomunikacji identyfikują zagrożenia systemów informatycznych oraz czy się przed nimi odpowiednio zabezpieczają.

Celem artykułu jest propozycja klasyfikacji źródeł zagrożeń systemów informatycznych oraz zbadanie, czy polskie przedsiębiorstwa identyfikują zagrożenia tych systemów. Badanie ma charakter pilotażu. Metodą badawczą przyjętą

w opracowaniu jest przegląd literatury, badań naukowych. Analizie poddano sprawozdania zarządu za lata 2019-2020 spółek notowanych na GPW w ramach indeksu WIG.

2. Podział źródeł zagrożeń systemów informatycznych

Klasyfikacje prezentowane przez polską i zagraniczną literaturę w zróżnicowany sposób ukazują źródła zagrożeń, na jakie jest narażony system informatyczny. Ich systematyzacja różni się szczególnie w zależności od rodzaju działalności prowadzonej przez przedsiębiorstwo. W dalszej części artykułu zaprezentowano niektóre z nich.

Ustalony przez E. Bompard et al. (2013, s. 53-55) podział dotyczy systemów energetycznych. Autorzy dzielą zagrożenia na naturalne, przypadkowe, złośliwe i nagłe. Z kolei w przypadkowych wyróżniają wewnętrzne i zewnętrzne, takie jak terroryzm, ewolucja systemów elektroenergetycznych czy innowacyjność technologii. Podają przykłady incydentów mających miejsce w różnym czasie i krajach. Zwracają również uwagę na ataki hakerskie oraz ataki fizyczne wymierzone w systemy informatyczne, a także infrastrukturę przedsiębiorstw m.in. z sektora energii i transportu. Kolejni autorzy ukazują złożoną, lecz schematyczną hierarchię źródeł zagrożeń systemów informatycznych (Jouinia, Ben Arfa Rabaia & Ben Aissab, 2014, s. 493-496). Prezentują wielowymiarowy podział, wychodząc od wewnętrznych i zewnętrznych, które w dalszej części dzielą na: ludzkie, środowiskowe i technologiczne, następnie na złośliwe i niezłośliwe dzielące się później na celowe i przypadkowe. Na koniec zaznaczają, że ich model jest ograniczony do binarnej dekompozycji źródeł zagrożeń.

Podział zaproponowany przez K. Schneidera (2012, s. 743-746) klasyfikuje zagrożenia ze względu na źródło (wewnętrzne − organizacyjne i technologiczne oraz zewnętrzne), celowość (przypadkowe i umyślne), rodzaj (oprogramowania i sprzętu) i wynik (całkowita utrata danych, kradzież informacji − wyciek danych), ingerencja w przetwarzane dane. Sklasyfikowane niebezpieczeństwa dotyczą systemu informatycznego księgowości.

Kolejny podział źródeł zagrożeń, z którymi można się spotkać w rachunkowości, został zaproponowany przez E. Szczepankiewicz (2017, s. 17-19). Autorka wyodrębnia celowe działania człowieka przeciwko zasobom informatycznym w rachunkowości zgodnie z klasyfikacją normy ISO/IEC TR 13335-3. Zalicza do nich m.in. umyślną szkodę lub zniszczenie, nielegalne używanie

oprogramowania, kradzież czy nieuprawnione użycie nośników. Następnie wyróżnia przestępczość komputerową jako przykład celowego działania w środowisku informatycznym, do której przydziela m.in.: haking, phishing, zarażenie systemu wirusami, niszczenie informacji, wewnętrzny lub zewnętrzny sabotaż komputerowy, kradzież danych/sprzętu, wandalizm. Wymienia czynniki ryzyka spowodowane niedoskonałością systemu kontroli zarządczej, dzieląc je na dwie grupy. Do pierwszej z nich zalicza: braki i/lub niedoskonałości zabezpieczeń fizycznych, technicznych i programowych dla zasobów informatycznych i/lub braki ubezpieczenia tych zasobów od zdarzeń losowych. W drugiej grupie umieszcza: braki i/lub niedoskonałe wewnętrzne procedury organizacyjno-administracyjne. Na koniec zwraca uwagę na istotny czynnik, jakim jest brak odpowiednich automatycznych procedur kontrolnych.

Następny podział źródeł zagrożeń bezpieczeństwa systemów informatycznych w finansach i rachunkowości zaprezentowali Ł. Siemieniuk, A. Gardocki & N. Siemieniuk (2018, s. 71-72). Podzielili zagrożenia na wewnętrzne (działania ludzi) i zewnętrzne (ataki hakerów na dane przechowywane na sprzętach elektronicznych). Autorzy skupili się na opisaniu ataków cyberprzestępców i hakerów.

Z kolei J. Madej & K. Szymczyk-Madej (2000, s. 168-170) przedstawili ogólną i opisową klasyfikację źródeł zagrożeń systemów informatycznych. Szczególną uwagę zwrócili na zagrożenia ataków hakerskich.

Klasyfikację źródeł zagrożeń systemu informatycznego przedstawił również J. Madej (2010, s. 83-84), w której podkreślił trudności w dokonywaniu jednoznacznego podziału. Wyróżnił w niej cztery kategorie: działania ludzi (przypadkowe i umyślne), awarie urządzeń i narzędzi informatycznych (sprzętu i oprogramowania), uchybienia i braki organizacyjne, zdarzenia losowe. Na podstawie tych elementów zaprezentował poszerzony katalog zagrożeń. Zdaniem autora może on stanowić podstawę do skonstruowania katalogu źródeł zagrożeń systemów informatycznych wykorzystywanego w praktyce.

Występują różnice w przedstawieniu klasyfikacji źródeł zagrożeń w 2000 roku oraz w 2010 roku. Jest to spowodowane wspomnianym rozwojem technologii, a wraz z nim metod dokonywanych włamań. Pokazuje to ewolucję w przedstawieniu rodzajów podłoży zagrożeń, która uwidoczniła charakter badanego obszaru podlegającego nieustannym zmianom. Stanowi również argument za cykliczną aktualizacją tych źródeł.

Kolejna klasyfikacja przedstawia źródła z punktu widzenia tzw. przestępczości komputerowej. Zawiera m.in. przywłaszczenie sobie autorstwa programu

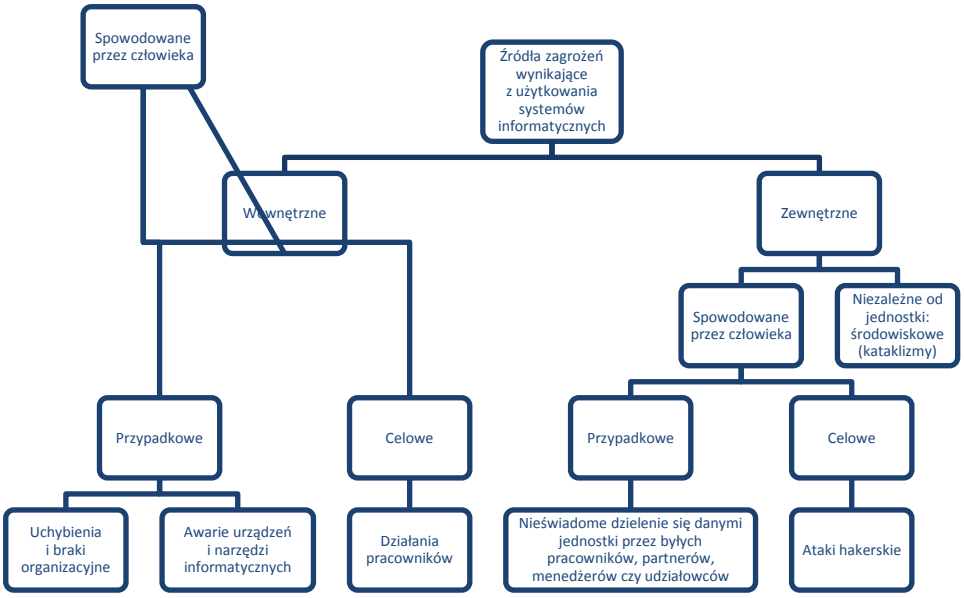
i jego fałszowanie, cracking (nieuprawnione wejście do systemu komputerowego), hacking (nieuprawniony dostęp do systemu komputerowego), przechwytywanie danych, phearing (oszustwa w systemach telekomunikacyjnych) (Kozioł, 2009, s. 7-10). Podział ten jest rozbudowany oraz wymienia numerycznie zagrożenia szeroko pojętej przestępczości komputerowej.

Według autora wspomniana transformacja cyfrowa i jej rosnące tempo zwiększone pandemią koronawirusa SARS-CoV-2, jak również powiększająca się ilość przetwarzanych danych wymuszają nieustanne podążanie za zmianami oraz aktualizację istniejących klasyfikacji źródeł zagrożeń systemów informatycznych.

3. Propozycja klasyfikacji źródeł zagrożeń systemów informatycznych

Analiza przedstawionych klasyfikacji pokazuje, że głównym źródłem zagrożenia systemów informatycznych jest człowiek, którego negatywnego oddziaływania nie sposób wyeliminować mimo zmieniających się warunków otoczenia, nowoczesnych technologii i postępu w dziedzinie informatyki. Człowiek może w różny sposób wpłynąć zarówno na działanie systemu, jak i bezpieczeństwo informacji. Z podobnego założenia wychodzi E. Szczepankiewicz (2017, s. 17), która w swojej klasyfikacji źródeł zagrożeń systemów informatycznych dodaje, że ludzie zagrażają systemom w sposób bezpośredni lub pośredni oraz losowy lub przypadkowy. W podziale K. Schneidera (2012, s. 743-746) brakuje szerszego opisania zagrożenia atakami hakerskimi. Klasyfikacja E. Szczepankiewicz (2017, s. 17) jest rozbudowana o wymieniony w niej m.in. phishing – zagrożenie, które wymaga szerszego wyjaśnienia.

W niniejszym opracowaniu za najbardziej właściwe kryterium podziału wskazano pochodzenie źródeł zagrożeń systemów. Wydaje się, że podział ten najlepiej porządkuje zróżnicowanie występujących zagrożeń oraz ich postrzeganie przez interesariuszy (rysunek 1).



Rysunek 1. Klasyfikacja źródeł zagrożeń wynikających z użytkowania systemów informatycznych w przedsiębiorstwie

Źródło: Opracowanie własne.

Przedstawiona klasyfikacja stanowi zestawienie istotnych źródeł zagrożeń, na jakie są narażone systemy informatyczne w przedsiębiorstwie. Punkt wyjścia stanowią źródła wewnętrzne i zewnętrzne, które następnie dzielą się na spowodowane przez człowieka i niezależne od jednostki − środowiskowe (zewnętrzne). Kolejny poziom to źródła przypadkowe i celowe. W podziale zwrócono szczególną uwagę na opis zagrożeń zewnętrznych, celowo spowodowanych przez człowieka – ataków hakerskich. Zdaniem autora jest to obecnie rosnący problem wielu jednostek gospodarczych.

Do celowych działań pracowników można zaliczyć:

- działanie pracownika na szkodę przedsiębiorstwa w celu osiągnięcia korzyści majątkowych;
- niszczenie informacji;
- nielegalne użytkowanie oprogramowania.

Natomiast do przypadkowych uchybień i braków organizacyjnych należą:

- nieodpowiednie i niewystarczające procedury postępowania lub całkowity brak zasad/wytycznych odnośnie do postępowania w danej sytuacji zagrożenia;
- niejasne rozdzielenie uprawnień i odpowiedzialności wśród pracowników;
- przekazywanie niewystarczających środków finansowych na szkolenia.

Do przypadkowych awarii urządzeń i narzędzi informatycznych należy zaliczyć:

- awarie hardware'u (np. serwerów, dysków twardych, płyty głównej);
- awarie software'u (np. systemu operacyjnego, oprogramowania, plików);
- awaria sieci komputerowej na skutek przerwy w dostawie energii elektrycznej.

Kolejne w zaprezentowanym podziale są ataki hakerskie stanowiące istotny rodzaj zagrożenia. Wynika to z wielu czynników, m.in. bagatelizowania przez przedsiębiorstwa (szczególnie te mniejsze) ryzyka ataku, uzależnienie współczesnych procesów od technologii i połączenia z siecią internetową, zdeterminowanie hakerów w osiągnięciu ich celów oraz często brak jakiegokolwiek przygotowania przedsiębiorstwa do ewentualnego ataku. W ostatnim czasie zagrożenia atakami hakerskimi stały się powszechne i bardziej niebezpieczne, a przez to wzrosło ryzyko znacznych strat finansowych dla przedsiębiorstw i osób fizycznych.

Do najpopularniejszych ataków hakerskich należy zaliczyć (Szpyra & Otwinowski, 2010, s. 77-89; Peszka, 2021):

- kradzież plików cookies;
- skrócone adresy;
- literówki w adresach www;
- fałszywe witryny i wyłudzanie danych;
- SQL Injection;
- wirusy komputerowe;
- przechwytywanie hasła w nieszyfrowanych protokołach;
- phishing.

Popularnym rodzajem ataku jest phishing. Hakerzy wykorzystują najczęściej niewiedzę lub naiwność pracowników. Celem jest kradzież informacji potrzebnych do logowania, szczegółów kart kredytowych czy innych wrażliwych danych. W tym celu haker podszywa się pod jedną ze stron w komunikacji internetowej – dla przykładu bank. Próba wyłudzenia informacji często sprowadza się do wysyłania wiadomości e-mail czy SMS do użytkowników danego banku z prośbą o podanie czy „potwierdzenie" pewnych danych. Użyte wiadomości przekierowują na stronę, która podszywa się pod prawdziwą witrynę instytucji. Niepodejrzewające podstępu osoby „weryfikują" na prośbę pewne dane czy też wykonują rutynową próbę logowania. W ten sposób haker uzyskuje dostęp do konta bankowego (Peszka, 2021). Pomimo, że o phishingu mówi się od jakiegoś czasu, to wiele osób, a tym samym przedsiębiorstw wciąż pada jego ofiarą. W celu uniknięcia przez jednostkę skutecznego ataku konieczne jest informowanie swoich pracowników o zagrożeniu i przeprowadzanie szkoleń.

Do źródeł zagrożeń niezależnych od jednostki, pochodzących z zewnątrz, należy zaliczyć przede wszystkim zagrożenia wynikające ze środowiska naturalnego – kataklizmy mogące wywołać przerwę w dostawie energii elektrycznej lub fizyczne zniszczenie serwerów.

Przypadkowe źródła zagrożeń spowodowane przez człowieka, pochodzące z zewnątrz to głównie nieświadome dzielenie się danymi jednostki przez byłych pracowników, partnerów, menedżerów czy udziałowców, a także wyciek danych jednostki ze strony interesariuszy, tj. dostawców i odbiorców czy instytucji publicznych.

W opracowaniu skupiono się głównie na systemach informatycznych, gdyż obecnie nie sposób rozpatrywać źródła zagrożeń z perspektywy wyłącznie jednego systemu, ponieważ w przypadku wystąpienia np. wycieku danych czy awarii sprzętu narażona jest cała jednostka gospodarcza. Jest to związane ze stopniem zaawansowania i skomplikowania samych systemów użytkowanych przez jednostki gospodarcze. Identyfikacja opisanych źródeł zagrożeń oraz sposoby zabezpieczania się przed nimi powinny być kluczowe dla prawidłowego funkcjonowania przedsiębiorstw.

4. Identyfikacja źródeł zagrożeń systemów informatycznych w sprawozdaniach zarządu spółek sektora transportu i logistyki

W celu zbadania, czy polskie spółki identyfikują źródła zagrożeń systemów informatycznych oraz czy podejmują działania zmierzające do ich niwelowania, poddano analizie sprawozdania zarządu spółek z sektora transportu i logistyki, energetycznego i telekomunikacyjnego notowanych na GPW w Warszawie z indeksu WIG.

Wybór sprawozdań zarządu był podyktowany ich powszechnym dostępem i obowiązkiem publikowania (zgodnie z art. 49 ust. 1 Ustawy o rachunkowości obowiązek sporządzania sprawozdania z działalności ciąży na kierowniku jednostki, m.in. spółek kapitałowych). Natomiast wybór spółek z indeksu WIG wynikał z jakości prezentowanych informacji. Spółki te są zazwyczaj grupami kapitałowymi, których wielkość obliguje do wysokiego poziomu zaangażowania w sporządzane raporty. Uzyskana próba badawcza stanowi osiemnaście sprawozdań zarządu wybranych spółek za lata 2019-2020, należących do branży

transportowej i logistycznej, energetycznej oraz telekomunikacyjnej, które obejmują wszystkie spółki z tego sektora notowane na GPW w Warszawie (GPW, 2021).

Sprawozdania zarządu publikowane przez spółki charakteryzują się zróżnicowanym poziomem jakości ujawnianych informacji, a także różnią się pod względem wizualnym. Część spółek prezentuje niewiele informacji mających na celu jedynie wypełnienie obowiązków wynikających z ustawy, a część sporządza obszerniejsze raporty (liczba stron waha się od 38 do 198). Warto również zaznaczyć, że spośród osiemnastu badanych spółek tylko trzy z nich (Tauron, Orange oraz PGE) sporządziły, poza sprawozdaniem zarządu, raport zintegrowany.

Wybrane informacje ze sprawozdań zarządu spółek na temat identyfikowanych źródeł zagrożeń systemów informatycznych i sposobów zabezpieczania się przed nimi przedstawia tabela 1.

Tabela 1. Wykaz informacji na temat źródeł zagrożeń systemów informatycznych w spółkach z sektora transportu i logistyki, energetycznego i telekomunikacyjnego w latach 2019-2020

Spółka	**Miejsce wykazania informacji o źródle zagrożeń**	**Wskazany obszar źródła zagrożeń (czy spółka identyfikuje ryzyko)**	**Podjęte działania przeciw źródłom zagrożeń lub jakie ujawnienia w SZ (jakie źródła identyfikuje i czy i jak się zabezpieczają)**
1	*2*	*3*	*4*
Enter Air S.A.	Brak	Brak	Brak
OT Logistic S.A.	Sprawozdanie zarządu (Oświadczenie o stosowaniu ładu korporacyjnego)	Główne cechy systemów kontroli zewnętrznej i zarządzania ryzykiem; prawidłowe prowadzenie ksiąg rachunkowych	• Ograniczenie dostępu do systemów informatycznych odpowiednimi uprawnieniami • Rozwiązania informatyczne i organizacyjne zabezpieczające kontrolę dostępu do systemu finansowo-księgowego oraz zapewniające należytą ochronę i archiwizację ksiąg rachunkowych
PGF Polska Grupa Fotowoltaiczna S.A. (dawniej Zastal S.A.)	Brak	Brak	Brak
PKP Cargo S.A.	Sprawozdanie zarządu (Oświadczenie o stosowaniu ładu korporacyjnego)	Prowadzenie ksiąg rachunkowych i stosowane polityki oraz rezultaty ich stosowania	• Bieżąca aktualizacja systemu finansowo-księgowego do wewnętrznych i zewnętrznych przepisów oraz wymogów sprawozdawczych • Ograniczenie dostępu do systemów informatycznych odpowiednimi uprawnieniami

cd. tabeli 1

1	*2*	*3*	*4*
			• Rozwiązania informatyczne i organizacyjne zabezpieczające kontrolę dostępu do systemu finansowo-księgowego oraz zapewniające należytą ochronę i archiwizację ksiąg rachunkowych • Funkcjonowanie Zintegrowanego Systemu Zarządzania (ZSZ) • W ramach ZSZ spółka dąży do: adekwatnych i proporcjonalnych zabezpieczeń zapewniających ochronę aktywom informacyjnym, wzrostu wiarygodności u klientów (zapewniając, że ich dane są bezpieczne), zapewnienia bezpieczeństwa i poufności informacji przetwarzanych w systemach teleinformatycznych, zapewnienia bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych, stałego monitoringu realizowanych procesów pod kątem bezpieczeństwa informacji, monitorowania skuteczności stosowanych zabezpieczeń oraz szybkiego reagowania na incydenty
Stalexport Autostrady S.A.	Brak	Brak	Brak
Trans Polonia S.A.	Brak	Brak	Brak
Enea	SZ	Wskazuje na ryzyka m.in.: ataku na infrastrukturę informatyczną, utraty ciągłości działania środowisk i infrastruktury teleinformatycznej, braku łączności z siecią Internet	• Przystąpienie do projektu zainicjowanego przez ministerstwo energii i podpisanie porozumienia dotyczącego współpracy sektora energetycznego na rzecz zwiększenia cyberbezpieczeństwa kraju (Tauron, Energa i PGE podpisały porozumienie). Dotyczy wspólnego działania w kierunku zwiększania bezpieczeństwa informatycznego obszaru dystrybucji energii oraz zabezpieczania go przed potencjalnymi atakami z zewnątrz • Doskonalenie systemu bezpieczeństwa teleinformatycznego i dostosowywanie go do nowych przepisów prawa • Wprowadzenie zaawansowanych rozwiązań informatycznych umożliwiających szybkie i sprawne reagowanie na incydenty cyberbezpieczeństwa oraz przeciwdziałających ryzykom z tego obszaru, ze szczególnym uwzględnieniem najnowszych zagrożeń, generowanych w związku z koniecznością dostosowania bezpieczeństwa systemów do pracy w okresie pandemii
Energa	SZ	Wskazuje ryzyko niedostosowania Grupy do nowych przepisów prawa oraz ryzyko bezpieczeństwa osób i mienia	• Grupy robocze ds. dostosowania działań Grupy do przepisów prawa • Potencjalne skutki ryzyka mogą się wiązać z zagrożeniem bezpieczeństwa pracy sieci, utratą/zniszczeniem mienia bądź przerwaniem ciągłości działania

cd. tabeli 1

1	*2*	*3*	*4*
			• Regulacje wewnętrzne z zakresu bezpieczeństwa • Monitoring incydentów dot. obszaru bezpieczeństwa w Grupie
Tauron	SZ	Wskazuje na ryzyko m.in.: utraty danych osobowych poprzez nieuprawniony dostęp, zwiększone ryzyko przez pandemię oraz wzrost liczby cyberataków	• Bezpieczeństwo: szczególny nacisk na bezpieczeństwo przetwarzania danych osobowych w systemach IT, implementowanie narzędzi i procedur zwiększenia cyberbezpieczeństwa • Wdrażanie i aktualizowanie procedur poprzez optymalizację bezpieczeństwa danych osobowych oraz szkolenia personelu w tym zakresie • Monitorowanie dostępu do informacji i zapewnienie środków jej ochrony
ML System	Brak	Brak	Brak
PGE	SZ	Wskazuje na ryzyko celowego zakłócenia prawidłowego funkcjonowania aktywów wytwórczych i dystrybucyjnych oraz systemów informatycznych funkcjonujących w GK PGE	Brak
Polenergia	Brak	Brak	Brak
ZEPAK	Brak	Brak	Brak
Kogeneracja	SZ	Wskazuje na ryzyko regulacyjno-prawne	• Zapewnienie adekwatnego poziomu bezpieczeństwa informacji, technologii teleinformatycznych oraz wywiązania się z obowiązków wynikających ze zmian w relewantnym otoczeniu regulacyjnym • Zapewnienie odpowiedniego procesu identyfikacji i reakcji na zagrożenia związane z cyberbezpieczeństwem • Opracowanie i wdrożenie odpowiednich procedur • Zastosowanie odpowiednich zabezpieczeń IT oraz OT
Będzin	Brak	Brak	Brak
Cyfrowy Polsat	SZ		• Rozwój kompetencji i usług z zakresu cyberbezpieczeństwa oraz szkolenia z zakresu cyberbezpieczeństwa • Technologia 5G – ma wspierać rozwój m.in. gospodarki 4.0 i cyberbezpieczeństwa • Nabycie pakietu akcji Asseco i dzięki temu wspólne działania na rzecz wpływania na kierunki rozwoju w perspektywicznych obszarach technologicznych (m.in. cyberbezpieczeństwa)

cd. tabeli 1

1	*2*	*3*	*4*
Orange	SZ	Wskazuje na ryzyko cyberaktaków, utraty dostępu do infrastruktury informatyczno-sieciowej	• Przyjęcie unijnego rozporządzenia *Cybersecurity act* i rozpoczęcie prac nad określeniem europejskich schematów certyfikacji cyberbezpieczeństwa; kwestie związane z certyfikacją elementów sieci 5G są rozważane do objęcia taką certyfikacją • Całodobowe reagowanie na zagrożenia, które napotykają użytkownicy Internetu za pomocą specjalnej jednostki CERT Orange Polska (wchodzi także w skład krajowego ekosystemu cyberbezpieczeństwa) • Odpowiednie planowanie rozwoju oraz modernizacja sieci i systemów teleinformatycznych, inwestowanie we wdrażanie rozwiązań przewidzianych na wypadek awarii, programy ubezpieczeniowe obejmujące zakresem ryzyka cybernetyczne i terrorystyczne, a także wdrażanie planów ciągłości działania i zarządzania kryzysowego
Netia	SZ	Brak	• Rozwój kompetencji oraz portfolio usług z zakresu cyberbezpieczeństwa • Budowa kompetencji integratorskich w ramach projektu NetiaNext (poszerzanie portfolio produktowego i szczególny nacisk na usługi cyberbezpieczeństwa) • Ochrona przed atakami na systemy komputerowe (DDoS), usługi kopii bezpieczeństwa danych (Backup as a Service), ochrona sieci IT za pomocą urządzeń firewall/UTM, usługi Security Operations Center

Źródło: Opracowanie własne.

Spośród sześciu spółek z sektora transportu i logistyki dwie z nich raportowały informacje na temat zabezpieczenia systemów informatycznych (OT Logistic i PKP Cargo). Natomiast spółki te nie identyfikowały w bezpośredni sposób źródeł zagrożeń. Głównym obszarem podlegającym zabezpieczeniom były programy finansowo-księgowe, a metodą zabezpieczania wprowadzenie autoryzacji i ograniczeń dostępu oraz bieżąca aktualizacja systemów informatycznych. Informacje te zostały ujęte w sprawozdaniach zarządu w części dotyczącej prowadzenia ksiąg rachunkowych. Stanowi to wąskie ujęcie zagrożeń systemów informatycznych i zabezpieczania się przed nimi. Ponadto w PKP Cargo funkcjonuje Zintegrowany System Zarządzania (ZSZ). Zabezpiecza on aktywa informacyjne jednostki, przyczynia się do wzrostu wiarygodności u klientów czy

bezpieczeństwa i poufności informacji przetwarzanych w systemach teleinformatycznych, zapewnienia bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych, stałego monitoringu realizowanych procesów pod kątem bezpieczeństwa informacji, monitorowania skuteczności stosowanych zabezpieczeń oraz szybkiego reagowania na incydenty.

Na wyróżnienie zasługuje PKP Cargo, która raportuje najwięcej informacji spośród spółek z badanego sektora o źródłach zagrożeń systemów informatycznych oraz sposobach zabezpieczania się przed nimi. Wprowadzony przez PKP Cargo ZSZ jest zorientowany na ciągłe doskonalenie oraz dostosowanie produktów do wymagań klientów i zobowiązuje spółkę do realizacji wysokiej jakości usług i zachowania bezpieczeństwa procesów. Ponadto ZSZ zobowiązuje pracowników m.in. do dbałości o bezpieczeństwo przetwarzanych informacji, przestrzegania zasad ich ochrony czy systematycznego szkolenia w zakresie bezpieczeństwa informacji. Spółka zauważa korzyści płynące z posiadania tego systemu, takie jak: pozytywne kształtowanie wizerunku firmy, wzrost prestiżu oraz zaufania, gwarancja wysokiej jakości świadczonych usług.

Spośród spółek z sektora energetycznego wyróżniają się Zespół Elektrociepłowni Wrocławskich Kogeneracja, Tauron, Energa oraz Enea. W ich sprawozdaniach zarządu znajduje się wiele informacji nt. cyberbezpieczeństwa i identyfikowanych ryzyk. Z kolei sektor telekomunikacyjny również odznacza się wysokim stopniem transparentności i raportuje o podjętych działaniach mających na celu zabezpieczenie przed cyberatakami, dokonanych inwestycjach (np. w technologię 5G również mającą się przyczynić do zwiększonego bezpieczeństwa).

5. Zakończenie

Zapewnienie bezpieczeństwa informacji przechowywanych przez systemy informatyczne może stanowić problem dla przedsiębiorstw. Niezabezpieczone lub nieprawidłowo zabezpieczone systemy mogą doprowadzić do strat finansowych. Przedstawiona w artykule klasyfikacja źródeł zagrożeń systemów informatycznych powstała w celu uzyskania porównywalności opisanych źródeł między różnymi systemami informatycznymi użytkowanymi w przedsiębiorstwach oraz ułatwienia przejmowania rozwiązań w zakresie zabezpieczeń z innych systemów informatycznych. To z kolei może służyć w odpowiednim doborze sposobów zabezpieczania się przed źródłami zagrożeń. Ponadto na podstawie klasyfikacji dokonano analizy sprawozdań zarządu spółek z sektora transportu i logistyki,

energetycznego i telekomunikacyjnego, aby sprawdzić, czy identyfikują źródła zagrożeń systemów informatycznych i jakiego doboru zabezpieczeń dokonują.

Uzyskane wyniki pokazują, że badane spółki mogą w rzeczywistości nie rozpoznawać wielu źródeł zagrożeń systemów informatycznych oraz nie zabezpieczać się przed nimi. Nie wyklucza to występowania sytuacji, w której przedsiębiorstwa te zabezpieczają się, lecz nie uwzględniają tych informacji w raportach. Nie zmienia to faktu, że brak informacji o źródłach zagrożeń systemów informatycznych oraz sposobów zabezpieczania się przed nimi znacząco obniża jakość sprawozdań, a w związku z tym powoduje spadek wiarygodności spółki dla jej interesariuszy. Potwierdza również potrzebę doskonalenia sporządzanych raportów i wzbogacenie ich o informacje niefinansowe. Przedsiębiorstwo poza danymi finansowymi powinno ujawniać istotne informacje, podobnie jak ujawnia wynik finansowy. Autor proponuje, aby badane spółki rozwijały obszar sprawozdawczości niefinansowej i uzupełniały sprawozdania zarządu, informacje dodatkowe oraz by podążały za nową formą raportowania − sprawozdawczością zintegrowaną. Ponadto spółki powinny dokonać przeglądu źródeł zagrożeń systemów informatycznych w swojej działalności oraz sposobów ich zabezpieczania, a następnie uwzględniać te informacje w sporządzanych sprawozdaniach zarządu bądź innych raportach niefinansowych. Działania te wpłyną na lepsze postrzeganie przez interesariuszy, co może się pośrednio przełożyć w dłuższej perspektywie na wyniki spółki i kurs akcji.

Należy również zaznaczyć, że stworzona klasyfikacja jest ograniczona z powodu mnogości i nieprzewidywalności występujących źródeł zagrożeń. W związku z tym ma charakter poglądowy i może stanowić bazę do budowy pełnej i zaawansowanej klasyfikacji, która stanowiłaby uniwersalny wzór dla przedsiębiorstw. Z kolei stosunkowo nieliczna grupa badanych spółek wynikała z niewielkiej liczby przedsiębiorstw z badanych sektorów. Badania miały charakter pilotażowy, ale mogą stanowić wstęp do pogłębionej analizy obejmującej sprawozdania zintegrowane.

Adrian Mencel – doktorant I roku dyscypliny Ekonomia i Finanse na Uniwersytecie Ekonomicznym w Katowicach. Od 2019 roku prezes Koła Naukowego Analiz Rynku Finansowego. Aktywnie uczestniczy w konferencjach naukowych. W dorobku posiada kilka prac naukowych. Równolegle od niemal 2 lat gromadzi doświadczenie w branży finansowej jako księgowy. Jego pasją jest fotografia cyfrowa – fotografia krajobrazowa oraz uprawianie biegów amatorskich na średnich dystansach.

Spis literatury

Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power and Energy Systems*, *50*, 50-64.

GPW. (2021). Pobrano z: https://www.gpw.pl/spolki (dostęp: 10.07.2021).

Jouinia, M., Ben Arfa Rabaia, L., & Ben Aissab, A. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.

Kozioł, M. (2009). Bezpieczeństwo informacji i ochrona systemów informatycznych w przedsiębiorstwie. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, *770*, 5-21.

Król-Stępień, M. (2013). System informatyczny rachunkowości jako narzędzie wspomagające zarządzanie jednostką gospodarczą – wymogi ustawowe a ich praktyczne stosowanie. *Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 757 Finanse, Rynki Finansowe, Ubezpieczenia*, *58*, 75-81.

Kunz, B., & Tymińska, A. (2014). System informatyczny rachunkowości i jego rola w świetle Ustawy o rachunkowości. *Nauki o Finansach*, *3*(20), 44-58.

Madej, J. (2010). Klasyfikacja zagrożeń bezpieczeństwa systemu informatycznego. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, *814*, 77-86.

Madej, J., & Szymczyk-Madej, K. (2009). Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach według kodeksu karnego, ustawy o rachunkowości i ustawy o ochronie danych osobowych. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, *770*, 109-122.

Madej, J., & Szymczyk-Madej, K. (2000). Bezpieczeństwo informatycznych systemów rachunkowości. *Zeszyty Naukowe Akademii Ekonomicznej w Krakowie*, *553*, 161-177.

Optimakers. (2021). Pobrano z: https://optimes.syneo.pl/blog/co-to-jest-system-erp/ (dostęp: 29.04.2021).

Peszka, D. (2021). *Jak wygląda atak hakerski na stronę www?* Pobrano z: https:// smartbees.pl/blog/jak-wyglada-atak-hakerski-na-strone-www (dostęp: 30.04.2021).

Schneider, K. (2012). Zagrożenia w systemie informatycznym rachunkowości. *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług*, *87* Gospodarka elektroniczna: wyzwania rozwojowe. T. 1, 740-748.

Siemieniuk, Ł., Gardocki, A., & Siemieniuk, N. (2018). Wybrane aspekty bezpieczeństwa systemów informatycznych w finansach i rachunkowości. *Przedsiębiorstwo & Finanse*, *4*, 69-78.

Szczepankiewicz, E. I. (2017). Zagrożenia dla zasobów informatycznych rachunkowości w dobie transformacji Information Technology w jednostkach sektora finansów publicznych. *Studia i Prace Kolegium Zarządzania i Finansów*, *157*, 9-30.

Szpyra, R., & Otwinowski W. (2010). Współczesne formy prowadzenia ataków informatycznych. *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa*, *3*, 77-90.

Ustawa z dnia 29 września 1994 r. o rachunkowości. Dz.U. z 2021 r. poz. 217. z późn. zm.

Podziękowania

Autor składa serdeczne podziękowania Pani dr Aleksandrze Ferens z Katedry Rachunkowości Uniwersytetu Ekonomicznego w Katowicach za wsparcie w zgłębianiu tematu w ramach Programu Tutoringu Akademickiego.

Threats resulting from the use of IT systems

Summary: Correct classification of threats to which IT systems used in enterprises are exposed may ensure the appropriate selection of methods of their protection. The creation of a homogeneous and consistent classification can lead to the comparability of the described threats between various IT systems used in enterprises. The uniform distribution of the sources of threats should also make it easier to take over security solutions from other IT systems. The aim of the article is to propose a classification of the sources of threats to information systems and to investigate whether Polish enterprises identify threats to these systems. The study is a pilot study. The research method adopted in the study is a review of literature, scientific research and an analysis of the management board reports of the surveyed 18 companies from the transport and logistics, energy and telecommunications sectors from the WIG index for 2019-2020. Based on the considerations, it should be stated that the presented classification allows to identify threats to information systems and may help in their protection. The analysis carried out in the article has shown that companies from the transport and logistics, energy and telecommunications sectors do not disclose little information about threats to IT systems occurring in their operations and related to them − ways of securing them. Companies from the energy sector reveal much more information, and companies from the telecommunications sector show the most.

Keywords: information systems, threats to information systems, classification of sources of threats to information systems.

JEL Classification: M15, M41, K24, L86.