SŁAWOMIR KUJAWA
PIOTR PISAREWICZ
https://doi.org/10.33995/wu2026.2.4
date of receipt: 21.01.2026
date of acceptance: 01.07.2026

Analiza produktów krajowych zakładów ubezpieczeń w zakresie cyberubezpieczeń w obliczu rosnących zagrożeń cybernetycznych dla sektora małych i średnich przedsiębiorstw oraz dla jednostek samorządu terytorialnego

Cyberzagrożenia są obecnie jednym z najpoważniejszych wyzwań dla sektora małych i średnich przedsiębiorstw (MŚP) oraz dla jednostek samorządu terytorialnego (JST) w Polsce. Brak rozbudowanych działów IT, ograniczone środki finansowe oraz niska świadomość w zakresie bezpieczeństwa informacyjnego sprawiają, że te podmioty często stają się łatwym celem cyberprzestępców. Sektor MŚP oraz JST w Polsce funkcjonują w środowisku, w którym liczba i złożoność zagrożeń cybernetycznych rośnie szybciej niż możliwości ich neutralizacji. Zakłady ubezpieczeń oferują produkty mające zabezpieczyć klientów przed negatywnymi skutkami naruszeń krytycznej infrastruktury cyfrowej (tzw. cyberubezpieczenia). Celem artykułu jest ocena adekwatności dostępnych na polskim rynku produktów cyberubezpieczeniowych do potrzeb sektora MŚP oraz dla JST poprzez identyfikację zakresu ochrony oferowanej przez krajowe zakłady ubezpieczeń i porównanie jej z charakterem oraz skalą współczesnych zagrożeń cybernetycznych. Dodatkowym celem jest identyfikacja ograniczeń podaży produktów cyberubezpieczeniowych oraz wskazanie obszarów wymagających dalszego rozwoju rynku.

Artykuł zawiera cztery rozdziały merytoryczne. W rozdziale pierwszym omówiono podstawy teoretyczne cyberbezpieczeństwa i zagrożeń cybernetycznych. Kluczowe zagrożenia cybernetyczne zostały opisane w rozdziale drugim, który – podobnie jak rozdział pierwszy – powstał na podstawie analizy krajowej i zagranicznej literatury przedmiotu. Rozdział trzeci zawiera empiryczną analizę produktów krajowych zakładów ubezpieczeń (w formie spółek akcyjnych – S.A. – oraz towarzystw ubezpieczeń

wzajemnych – TUW) w zakresie cyberubezpieczeń oferowanych małym i średnim przedsiębiorstwom oraz jednostkom samorządu terytorialnego. Rozdział czwarty przynosi wnioski z analizy OWU proponowanych przez ubezpieczycieli.

Wyniki badań wskazują na ograniczoną liczbę dedykowanych produktów cyberubezpieczeniowych w Polsce, znaczące zróżnicowanie zakresu ochrony oraz brak ich pełnego dopasowania do struktury zagrożeń identyfikowanych w obu sektorach. Wnioski z analizy mogą stanowić podstawę do dalszych działań regulacyjnych, edukacyjnych i rozwojowych w obszarze cyberubezpieczeń w Polsce.

Słowa kluczowe: zakłady ubezpieczeń, MŚP, JST, cyberbezpieczeństwo, cyberryzyko, usługi ubezpieczeniowe

Wprowadzenie

Technologie informacyjno-komunikacyjne (ICT) są obecnie podstawowym narzędziem wykorzystywanym przez instytucje finansowe oraz niemal wszystkie sektory gospodarki. Dzięki nim rynki, podmioty gospodarcze i instytucje finansowe zwiększyły w sposób znaczący zakres i zasięg oferowanych usług oraz produktów. Ponadto, wiele innych obszarów funkcjonowania opartych jest o wszelkiego rodzaju aplikacje i rozwiązania teleinformatyczne. Przykłady można by mnożyć: są to transport, przemysł, logistyka, media itp. – trudno w zasadzie znaleźć obszar, który funkcjonuje bez tego rodzaju wsparcia. Swoiste uzależnienie od nowych technologii i wzrost wzajemnych powiązań w skali globalnej spowodowały jednak wzrost ryzyka związanego ze stosowaniem technologii ICT. Społeczeństwo, system finansowy, jak również pozostałe sektory gospodarki, stały się bardziej podatne na wszelkiego rodzaju cyberzagrożenia i problemy z nich wynikające.

Sektor finansowy pozostaje w czołówce celów cyberataków na świecie. Podobnie jest w Polsce, gdzie po sektorze bankowym, który jest głównym celów cyberataków, kolejnymi są administracja publiczna (w tym jednostki samorządu terytorialnego), sektor energetyczny, sektor dóbr konsumpcyjnych, handel internetowy (e-commerce), sektor IT oraz farmaceutyczny[1]. Typowe cyberzagrożenia ubezpieczycieli w mniejszym lub większym stopniu dotyczą również ich klientów, czyli omawianych w niniejszym opracowaniu małych i średnich przedsiębiorstw (MŚP oraz JST). Należą do nich w szczególności[2]:

- utrata i/lub kradzież poufnych danych, zagrażające bezpieczeństwu klientów, pracowników, współpracowników i partnerów biznesowych;
- phishing, czyli wyłudzanie danych, dostępu do systemów i/lub informacji za pomocą rozsyłania informacji e-mail zawierających łącza internetowe do złośliwego oprogramowania;
- ransomware, czyli oprogramowanie szyfrujące bazy danych i wymuszające okup;

1. Vecto, *Cyberbezpieczeństwo w polskich firmach. Raport 2020*, 2020, https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2020.pdf [dostęp: 18.12.2025].
2. EIOPA, *Cyber risk for insurers – challenges and opportunities* 2019, 2019, European Insurance and Occupational Health Pension Authority, https://www.eiopa.europa.eu/document/download/61701869-eab9–49c7-a9ec-14d0b810f755_en?filename=Cyber%20Risk%20for%20Insurers%20-%20Challenges%20and%20Opportunities [dostęp: 18.12.2025].

- cryptojacking, to jest włamania do sprzętowych zasobów informatycznych (hardware) w celu wykorzystania ich mocy obliczeniowych przez „kopalnie kryptowalut";
- DDoS (ang. *Distributed Denial of Service*) – ataki, mające uniemożliwić działanie systemów komputerowych lub usług sieciowych przez zajęcie bądź zablokowanie wszystkich zasobów;
- SQL Injection, czyli atak cybernetyczny polegający na wstrzyknięciu razem z danymi formularza na stronie internetowej fragmentu zapytania do bazy danych w celu wykradzenia jej treści lub manipulacji zawartością;
- zero day exploit, czyli wykorzystanie luki w oprogramowaniu, która nie została jeszcze rozpoznana przez jego twórców i dla załatania której nie została jeszcze udostępniona aktualizacja;
- nieautoryzowane transakcje i kradzieże funduszy;
- cyberataki i problemy z systemami informacyjnymi w łańcuchach dostaw i w organizacjach partnerów biznesowych.

Współczesne organizacje, niezależnie od swojej wielkości czy charakteru działalności, funkcjonują w środowisku silnie uzależnionym od technologii cyfrowych. Cyfryzacja procesów biznesowych, administracyjnych i komunikacyjnych przynosi liczne korzyści, ale równocześnie generuje nowe ryzyka. Cyberzagrożenia są obecnie jednym z najpoważniejszych wyzwań dla sektora MŚP oraz dla JST w Polsce. Brak rozbudowanych działów IT, ograniczone środki finansowe oraz niska świadomość w zakresie bezpieczeństwa informacyjnego sprawiają, że te podmioty często stają się łatwym celem cyberprzestępców. Sektor MŚP oraz JST w Polsce funkcjonują w środowisku, w którym liczba i złożoność zagrożeń cybernetycznych rośnie szybciej niż możliwości ich neutralizacji. Raporty krajowych i międzynarodowych instytucji – w tym CERT Polska[3], NASK[4], ENISA[5], KPMG[6], Ministerstwa Cyfryzacji[7], Check Point Research[8], PwC[9], Fortinet[10], Orange Polska[11], Business Insider[12] oraz ESET[13] wskazują, że organizacje w Polsce w 2024 roku stały się szczególnie narażone na ataki ukierunkowane, zautomatyzowane i wykorzystujące jednocześnie ich słabości organizacyjne, w tym kadrowe i infrastrukturalne.

3. CERT Polska, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2024*, 2025, https://cert.pl [dostęp: 17.12.2025].
4. NASK, *Raport roczny z działalności CERT Polska*, 2024, https://nask.pl [dostęp: 17.12.2025].
5. ENISA, *Threat Landscape 2024 (Poland section)*, 2024, https://www.enisa.europa.eu/topics/threat-landscape [dostęp: 17.12.2025].
6. KPMG Polska, *Barometr cyberbezpieczeństwa 2024*, 2024, https://kpmg.com/pl [dostęp: 17.12.2025].
7. Ministerstwo Cyfryzacji, *Cyberbezpieczny samorząd 2024*, 2024, https://www.gov.pl/cyfryzacja [dostęp: 17.12.2025].
8. Check Point Research, *Cyber Security Report Poland 2024*, 2024, https://www.checkpoint.com [dostęp: 17.12. 2025.]
9. PwC, *Global Digital Trust Insights 2026*, www.pwc.com [dostęp: 17.12.2025].
10. Fortinet, *Global Threat Landscape Report 2025 (Poland Highlights)*, 2025, https://www.fortinet.com [dostęp: 17.12.2025].
11. Orange Polska, *CyberTarcza: raport bezpieczeństwa 2024*, 2024, https://www.orange.pl/bezpieczenstwo [dostęp: 17.12.2025].
12. Business Insider, *Zarządzaj ryzykiem, nie kryzysem. Przewodnik po skutecznym cyberbezpieczeństwie dla firm*, 2024, https://businessinsider.com.pl/technologie/nowe-technologie/zarzadzaj-ryzykiem-nie-kryzysem--raport-o-cyberbezpieczenstwie-dla-firm-pobierz/4rfetwg [dostęp: 6.01.2026].
13. ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*, 2025, https://in.eset.pl/ [dostęp: 17.12.2025].

Kluczowym wyzwaniem najbliższej przyszłości jest zatem zapewnienie odporności cyfrowej, bezpieczeństwa oraz wynikającej z nich jakości świadczonych usług. Sektor ubezpieczeń pełni tutaj podwójną rolę. Z jednej strony opiera swoją działalność na przetwarzaniu wielkich ilości informacji – są to dane o charakterze zarówno osobowym, jak i nieosobowym[14]. Zastosowanie technologii cyfrowych obejmuje niemal wszystkie obszary działalności zakładów ubezpieczeń: zarządzanie produktem, wycena, underwriting, sprzedaż i dystrybucja, likwidacja szkód itp.[15] Drugim obszarem aktywności ubezpieczycieli jest oferowanie klientom produktów mających zabezpieczyć ich przed negatywnymi skutkami wynikającymi z naruszeń krytycznej infrastruktury cyfrowej (tzw. cyberubezpieczenia). Ten wątek rozważań – nakierowanie na propozycję produktową ubezpieczycieli skierowaną do małych i średnich przedsiębiorstw oraz jednostek samorządu terytorialnego – stanowi główny punkt ciężkości niniejszego artykułu. Celem analizy jest ocena adekwatności dostępnych na polskim rynku produktów cyberubezpieczeniowych dla sektora MŚP oraz JST poprzez identyfikację zakresu ochrony oferowanej przez krajowe zakłady ubezpieczeń i zestawienie jej z charakterem oraz skalą współczesnych zagrożeń cybernetycznych. Dodatkowym celem jest identyfikacja ograniczeń podaży produktów cyberubezpieczeniowych oraz wskazanie obszarów wymagających dalszego rozwoju rynku.

W rozdziale pierwszym artykułu omówiono podstawy teoretyczne cyberbezpieczeństwa i zagrożeń cybernetycznych. Kluczowe zagrożenia cybernetyczne zostały opisane w rozdziale drugim, który – podobnie jak rozdział poprzedni – powstał na podstawie analizy krajowej i zagranicznej literatury przedmiotu. Rozdział trzeci zawiera empiryczną analizę produktów krajowych zakładów ubezpieczeń (w formie S.A. oraz TUW) w zakresie cyberubezpieczeń dla sektora MŚP i JST. Rozdział czwarty – wnioski z analizy ogólnych warunków ubezpieczenia.

Usługi świadczone przez zakłady ubezpieczeń muszą być oferowane z zachowaniem najwyższych norm jakości i bezpieczeństwa wynikających zarówno z regulacji prawnych, jak i ze standardów narzuconych przez sam rynek. Aby spełnić te wymogi, podmioty stosują szereg procedur, które mają być zgodne z literą, a niejednokrotnie z „duchem" ustawy, jako że niektóre jej zapisy wydają się dosyć ogólne. W tym właśnie celu polski organ nadzoru – Komisja Nadzoru Finansowego (KNF) na mocy przepisów ustawowych[16], uchwala bardziej szczegółowe dokumenty, których intencją jest doprecyzowanie zapisów ustawowych oraz osiągnięcie maksymalnego stopnia jakości i bezpieczeństwa (wytyczne, rekomendacje). Pozwalają one uniknąć szeregu negatywnych skutków wynikających z ryzyka operacyjnego, które może zmaterializować się w formie straty wynikającej z niewłaściwych lub błędnych procesów wewnętrznych, działań personelu, systemów i zdarzeń zewnętrznych. Część wytycznych i rekomendacji czyli tzw. aktów miękkiego prawa dotyczących szeroko pojętego bezpieczeństwa technologii ICT, została uchylona i w dniu 17 stycznia 2025 roku zastąpiona przez nowy jednolity akt prawny uchwalony na poziomie Unii

14. A. Małek, J. Monkiewicz, M. Monkiewicz, *Ubezpieczenia w świecie cyfrowym: nowe uwarunkowania i wyzwania*, [w:] *Ubezpieczenia cyfrowe: możliwości, oczekiwania, wyzwania*, [red.] J. Monkiewicz, L. Gąsiorkiewicz, P. Gołąb, M. Monkiewicz, PWN, Warszawa 2022.
15. J. Monkiewicz, M. Monkiewicz, *Ubezpieczenia w świecie cyfrowym: nowe wyzwania*, [w:] J. Monkiewicz, L. Gąsiorkiewicz, *Finanse cyfrowe. Perspektywa rynkowa*, Wydawnictwo Politechniki Warszawskiej, Warszawa 2021, s. 74.
16. Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. 2024, poz. 838, 1565, 1863), art. 365 ust. 1.

Europejskiej[17]. Jest to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 roku w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Rozporządzenie DORA). Jego głównym zadaniem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług ICT na rynku finansowym – w tym w sektorze ubezpieczeń. Wdrożenie przepisów Rozporządzenia DORA ma umożliwić udoskonalenie i rozwój otoczenia regulacyjnego w obszarze nowych technologii oraz harmonizację procedur i standardów dotyczących odporności cyfrowej w sektorze finansowym. Finalnym efektem wdrożenia dokumentu ma być wzrost odporności podmiotów sektora finansowego na zakłócenia operacyjne, przerwanie ciągłości działania, cyberataki i zagrożenia związane z technologiami informacyjno-komunikacyjnymi. Rozporządzenie ujednolica przepisy we wszystkich państwach członkowskich UE, obejmując podmioty działające na rynku finansowym: banki, zakłady ubezpieczeń, firmy inwestycyjne, instytucje płatnicze, jak również dostawców technologii i usług ICT. Nakłada ono na podmioty obowiązek rejestrowania i klasyfikowania incydentów wpływających na stabilność, ciągłość lub jakość usług finansowych. Jest to ważne ogniwo w złożonej architekturze nowych wymogów regulacyjnych, których implementacja ma się przyczynić do zwiększenia odporności cyfrowej, a tym samym – bezpieczeństwa i jakości świadczonych usług. Wszechobecność narzędzi cyfrowych i nowe wymogi regulacyjne identyfikują bezpieczeństwo cyfrowe jako ważny aspekt działalności zakładów ubezpieczeń. W najbliższych latach oba te czynniki powinny przyczynić się do poprawy jakości, zakresu oraz adekwatności produktów ubezpieczycieli skierowanej do klientów – w tym omawianych w niniejszym artykule podmiotów z sektora MŚP i JST.

Problematyka poruszana w artykule obok aspektów teoretycznych ma również zastosowanie praktyczne. Autorzy niniejszego opracowania wyrażają nadzieję, iż ujęcie w nim zaproponowane przedstawia omawiane zagadnienia z innej, nie poruszanej dotychczas perspektywy.

1. Podstawy teoretyczne cyberbezpieczeństwa i zagrożeń cybernetycznych

Cyberbezpieczeństwo może być definiowane przez pryzmat różnych zagrożeń, które niesie za sobą rozwój cyberprzestrzeni i funkcjonowanie w niej poszczególnych użytkowników. Samo pojęcie cyberprzestrzeni nie jest łatwe do uchwycenia z powodu niezwykle szybkiego rozwoju sfery informacyjnej, w tym przede wszystkim internetu i obszarów w różnym stopniu z nim związanych, takich jak internet rzeczy (IoT, ang. *Internet of Things*), big data, cloud computing, robotyka, czy wreszcie rozwój sztucznej inteligencji (AI, ang. *Artificial Intelligence*)[18]. Jedna z definicji cyberprzestrzeni sformułowana przez Departament Obrony USA jest następująca: „[...] globalna

17. KNF, *Komunikat KNF: Planowane uchylenie rekomendacji i wytycznych dot. zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego oraz odwołanie komunikatu chmurowego w związku z rozpoczęciem stosowania Rozporządzenia DORA*, 2024, https://www.knf.gov.pl/?articleId=91751&p_id=18 [dostęp: 17.01.2025].

18. J. Podlewski, *Wdrażanie koncepcji sztucznej inteligencji w polskiej gospodarce. Problemy i rozwiązania*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2021.

domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesy oraz kontrolery"[19]. W polskim prawodawstwie cyberprzestrzeń zdefiniowana jest w sposób następujący: „[…] przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami"[20]. W przywołanym wyżej akcie prawnym systemy teleinformatyczne zdefiniowane są z kolei jako: „[…] zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów Ustawy z dnia 12 lipca 2024 roku – Prawo komunikacji elektronicznej[21]". Tytułem uzupełnienia: telekomunikacyjne urządzenie końcowe to „urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończenia sieci[22]".

Doktryna cyberbezpieczeństwa RP definiuje cyberprzestrzeń jako „przestrzeń przetwarzania i wymiany informacji tworzonych przez systemy teleinformatyczne" a wspomniane już cyberbezpieczeństwo jako „proces zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni"[23]. Ten rządowy dokument jest elementem regulacyjnego i strategicznego[24] podejścia do bezpieczeństwa cybernetycznego, odgrywa na całym świecie niezwykle ważną rolę. Szeroko rozumiane ryzyko cybernetyczne nosi znamiona ryzyka systemowego. Zagrożenia cyberbezpieczeństwa w wielu aspektach wpływają pośrednio i bezpośrednio na jakość świadczonych usług[25]. Przykładem bezpośredniego oddziaływania na codzienne operacje, w tym na bieżącą obsługę klienta, są zakłócenia w działalności systemów informatycznych wywoływane cyberatakami. W skrajnych wypadkach (np. ataki typu DDOS czy przejęcie systemów informatycznych przez oprogramowanie ransomware) może dojść do opóźnienia bądź przerwania możliwości obsługi klientów nawet na długi okres[26]. Pośrednie, długofalowe oddziaływanie takich zdarzeń wykracza poza bezpośrednie, bieżące koszty

19. K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2025, nr 1(13).
20. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. 2002, nr 156, poz.. 1301), art.2.1b.
21. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2024, poz. 1557 i 1717 z późn. zm.), art. 3 pkt.3.
22. Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, (Dz. U. 2024,. poz. 1221; Dz. U. 2025, poz.. 637, 820, art.2 pkt. 71).
23. Biuro Bezpieczeństwa Narodowego, *Doktryna bezpieczeństwa Rzeczpospolitej Polskiej*, Warszawa 2015.
24. K. Chochowski, *Strategia cyberbezpieczeństwa jako przejaw polityki administracyjnej*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Seria Prawnicza" 2019, z. 107.
25. *Cyber risks: what is the impact on the insurance industry?*, *European Insurance and Occupational Health Pension Authority*, EIOPA, 2021, https://www.eiopa.europa.eu/cyber-risks-what-impact-insurance-industry-2021-10-15_en [dostęp: 20.12.2025].
26. B. Moorcraft, *CNA concludes investigation into cyberattack*, "Insurance Business" 2021, https://www.insurancebusinessmag.com/ca/news/cyber/cna-concludes-investigation-into-cyberattack-260688.aspx [dostęp: 28.12.2025].

finansowe (usuwanie awarii, zapłata okupu). Naruszenia cyberbezpieczeństwa mogą osłabiać zaufanie klientów do jakości świadczonych usług deklarowanych przy zawieraniu umów i podważać reputację ubezpieczyciela. W efekcie w negatywny sposób wpływać mogą na wyniki finansowe i pozycję rynkową podmiotu[27]. Biorąc pod uwagę powyższe kwestie, konieczne staje się potraktowanie bezpieczeństwa cybernetycznego nie tylko z punktu widzenia bezpiecznego i niezakłóconego działania firmy, ale także, a może przede wszystkim z punktu widzenia wartości dla klienta.

Ważnym wątkiem badanych kwestii są również szkody powodowane w cyberprzestrzeni i skala strat z nimi związanych. Szkody tego typu można podzielić ze względu na relacje podmiotowe, w których występuje strata. Pierwszym przypadkiem jest ryzyko utraty własnych aktywów (*first party risk*), gdy sam podmiot na skutek cyberataku ponosi wysokie koszty powodujące stratę. Drugi scenariusz to ryzyko utraty aktywów podmiotów powiązanych (*second party risk*). Występuje ono nie tylko wtedy, gdy podmioty są powiązane kapitałowo, ale także w przypadku, gdy między podmiotem bezpośrednio dotkniętym cyberatakiem a innym istnieje relacja kontraktowa. I wreszcie ostatnia sytuacja, w której materializuje się ryzyko związane z odpowiedzialnością wobec osób trzecich (*third party risk*), czego przejawami mogą być m.in. kradzieże pieniędzy z rachunków bankowych lub kradzieże danych osobowych klientów[28].

Kolejnym wątkiem, który w części teoretycznej wymaga doprecyzowania, jest ryzyko cybernetyczne będące podstawą każdego produktu ubezpieczeniowego w obszarze cyberubezpieczeń. Ryzyko cybernetyczne jest różnie definiowane, niemniej w odmiennych wyjaśnieniach znajdziemy wiele cech wspólnych. Poniżej przywołano wybrane definicje, które w opinii autorów artykułu oddają należycie istotę badanych kwestii. Pierwsza z nich tłumaczy cyberryzyko jako: „jakiekolwiek ryzyko wynikające z wykorzystania technologii informacyjno-komunikacyjnych, które narusza poufność, dostępność lub integralność danych lub usług"[29]. Nieco inne podejście wskazane jest w kolejnej definicji: „wszelkie ryzyka wynikające z wykorzystania danych elektronicznych i ich transmisji, w tym narzędzi technologicznych, takich jak internet i sieci telekomunikacyjne"[30]. Ryzyko cybernetyczne jako ryzyko wystąpienia szkodliwych zdarzeń elektronicznych, które powodują zakłócenia w działalności przedsiębiorstwa lub straty finansowe, jest przykładem syntetycznego ujęcia tego zagadnienia[31]. Kolejna możliwa definicja ukazuje ryzyko cybernetyczne jako ryzyko operacyjne w sferze zasobów informacyjnych i technologicznych danej organizacji, którego skutki o charakterze negatywnym mogą oddziaływać na poufność, dostępność oraz integralność informacji bądź systemów informatycznych[32]. Inne syntetyczne podejście zaproponowane zostało przez specjali-

27. CSFI, *Insurance banana skins 2023. The CSFI survey on the risk facing insurers*, The Centre for the Study of Financial Innovation, London 2023, https://www.pwc.co.uk/insurance/assets/pdf/insurance-banana-skins-2023.pdf [dostęp: 20.12.2025].
28. K. Malinowska, *Aspekty prawne ubezpieczenia cyber ryzyk*, „Prawo Asekuracyjne" 2018, nr 2(95), s.. 20.
29. The Geneva Association, *Ten Key Questions on Cyber Risk and Cyber Risk Insurance*, Zurich 2016, [za:] *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris 2017, s. 20.
30. Chief Risk Officers – CRO Forum, *Cyber resilience: The cyber risk challenge and the role of insurance*, Amsterdam, www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf, [za:] *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris 2017, s. 20.
31. A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S. Sadhukhan, *Cyber-risk decision models: To insure IT or not?*, "Decision Support Systems" 4/2013, http://dx.doi.org/10.1016/j.dss.2013.04.004 [dostęp: 11.12.2025].
32. J.J. Cebula, L.R. Young, *A taxonomy of operational cyber security risks*, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, Pittsburgh 2010.

stów z międzynarodowej firmy brokerskiej Marsh. Cyberryzyko to według nich ryzyko gospodarcze związane z posiadaniem, działaniem, wykorzystaniem i oddziaływaniem urządzeń i technologii IT w przedsiębiorstwie[33]. Ryzyko cybernetyczne przedstawione jako niebezpieczeństwo zakłócenia systemów informacyjnych[34] lub jako ryzyko naruszenia bezpieczeństwa informacji[35] to kolejne próby bardzo ogólnego i syntetycznego zdefiniowania omawianych zagadnień. Nieco szerzej rodzaje cyberryzyka oraz jego skutków opisuje organ nadzoru nad rynkiem ubezpieczeń w USA. W jego ujęciu mogą to być: kradzieże tożsamości, przerwy w działalności spowodowane awariami systemów komputerowych, utrata reputacji, odtworzenie danych utraconych w wyniku cyberataku oraz związane z tym koszty, kradzieże poufnych informacji handlowych, infekcje złośliwym oprogramowaniem, nieuprawnione ujawnianie danych poufnych spowodowane błędami ludzkimi, naruszanie bezpieczeństwa danych osobowych i praw autorskich oraz związane z nimi koszty[36].

Nawiązując do skutków materializacji cyberryzyka, istotne dla dalszych rozważań będzie również zdefiniowanie i umiejscowienie cyberubezpieczeń na tle innych rodzajów produktów ubezpieczeniowych. Najbardziej precyzyjne będzie zakwalifikowanie ich pod względem przedmiotowym do odpowiedniej grupy ryzyka w Dziale II ubezpieczeń[37]. Sprawa jest bardzo złożona i interesująca zarazem, ponieważ w zależności od rodzaju możliwej szkody, można zakwalifikować je do:„[…] grupy 9 – ubezpieczenia pozostałych szkód rzeczowych (jeżeli nie zostały ujęte w grupach 3, 4, 5, 6 lub 7), wywołanych przez grad lub mróz oraz inne przyczyny (jak np. kradzież), jeżeli przyczyny te nie są ujęte w grupie 8; grupy 13 – ubezpieczenia odpowiedzialności cywilnej (ubezpieczenie odpowiedzialności cywilnej ogólnej) nieujętej w grupach 10–12; a wreszcie do grupy 16 – ubezpieczenia ryzyk finansowych, w tym: m.in. utraty zysków, stałych wydatków ogólnych, nieprzewidzianych wydatków handlowych oraz innych strat finansowych; grupy 17 – ubezpieczenia ochrony prawnej"[38].

Podsumowując zagadnienia teoretyczne, należy jeszcze zdefiniować rodzaje zagrożeń cybernetycznych. Wspomniane wcześniej cyberzagrożenia dzieli się zwykle na trzy obszary: techniczne, socjotechniczne i organizacyjne. Zagrożenia techniczne obejmują złośliwe oprogramowanie (malware), trojany, ransomware oraz ataki na infrastrukturę, takie jak DDoS lub wykorzystanie podatności systemowych. Przykładowo, ataki ransomware – stanowiące jedno z najgroźniejszych zagrożeń – w 2024 roku najczęściej dotykały firmy, ale także instytucje publiczne i osoby

33. *UK cyber security. The role of insurance in managing and mitigating the risk*, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/ file/415354/UK_Cyber_Security_Report_Final.pdf [dostęp: 11.12.2025].
34. R. Böhme, G. Kataria, *Models and measures for correlation in cyber-insurance*, Working Paper, Workshop on the Economics of Information Security (WEIS), University of Cambridge, Cambridge 2006, http://www.econinfosec.org/archive/weis2006/docs/16.pdf [dostęp: 11.12.2025].
35. H. Ögűt,, S. Raghunathan,, N. Menon, *Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection*, "Risk Analysis" 2011, No. 31(3), doi: 10.1111/j.1539–6924.2010.01478.x [dostęp: 11.12.2025].
36. National Association of Insurance Commissioners – NAIC, *Cybersecurity*, USA, 2016; za: G. Strupczewski, *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie*, „Finanse. Czasopismo Komitetu Nauk o Finansach PAN" 2017, nr 1(10), s. 253.
37. Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, (Dz. U. 2024, poz. 838, 1565, 1863), załącznik.
38. K. Malinowska, *Aspekty prawne ubezpieczenia cyber ryzyk* …, s. 21.

prywatne[39]. Zagrożenia socjotechniczne wynikały z manipulacji użytkownikami, przede wszystkim za pomocą phishingu, smishingu i oszustw w mediach społecznościowych. Eksperci podkreślają, że przestępcy coraz częściej porzucają „bardzo techniczne" metody na rzecz inżynierii społecznej, wykorzystując np. fałszywe wezwania od policji, podszywanie się pod dziecko na WhatsApp czy złośliwe kody QR[40]. Zagrożenia organizacyjne obejmują natomiast braki formalnych procedur, niską dojrzałość organizacyjną, brak analiz ryzyka i niewystarczające zasady kontroli dostępu.

Wszystkie rodzaje zagrożeń, ryzyko oraz potencjalne szkody wynikające z jego materializacji znajdują w mniejszym lub większym stopniu swoje odzwierciedlenie w zakresie poszczególnych produktów zakładów ubezpieczeń, które zostały poddane analizie w dalszej części niniejszego opracowania.

2. Kluczowe zagrożenia cybernetyczne w sektorze MŚP i w JST

Pomimo działającej od wielu lat Ustawy o krajowym systemie cyberbezpieczeństwa oraz obowiązujących standardów dotyczących cyberbezpieczeństwa[41],[42], w sektorze MŚP oraz w licznych JST wciąż dominuje działanie *ad hoc*. Podmioty tych sektorów funkcjonują często bez wdrożonego systemu zarządzania bezpieczeństwem informacji — na co wskazuje poradnik pt. *Cyberbezpieczny samorząd*[43]. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający w strukturach NASK-PIB (CSIRT NASK), w 2024 roku odnotował rekordowy wzrost aktywności cyberprzestępców. Liczba zgłoszeń wyniosła 600 990 (wzrost o 62% w porównaniu z rokiem 2023), a liczba zarejestrowanych incydentów zwiększyła się o 29%. Średnia miesięczna liczba zgłoszeń wyniosła natomiast około 50 tysięcy. Ten wzrost wynika nie tylko z większej aktywności cyberprzestępców, ale także z rosnącej świadomości zagrożeń w sieci[44]. Analizy incydentów w Polsce wskazują na kilka dominujących typów ataków, których liczebność i udział procentowy można przybliżyć danymi z raportów krajowych. Poniżej ich zestawienie.

- Phishing i oszustwa sieciowe: to najczęstszy sposób ataku. CERT Polska raportuje, że oszustwa komputerowe stanowią 94,7% wszystkich zgłoszonych incydentów (97 995), przy czym phishing odpowiada za 40 120 przypadków[45]. W sektorze telekomunikacyjnym operatorzy telefonii komórkowej (np. Orange) blokują setki tysięcy domen phishingowych – w 2024 roku Orange odnotował blokadę 305 tys. fałszywych stron, chroniąc tym samym 4,85 mln osób[46].

39. CERT Polska, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2024*, 2025, https://cert.pl [dostęp: 17.12.2025].
40. NASK, *Raport roczny z działalności CERT Polska*, 2024, https://nask.pl [dostęp: 17.12.2025].
41. ISO/IEC, ISO/IEC 27032:2023 Information security, cybersecurity and privacy protection – Guidelines for cybersecurity, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), Geneva 2023.
42. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (Dz. U. 2018, poz. 1560).
43. Ministerstwo Cyfryzacji, *Cyberbezpieczny samorząd 2024*…
44. NASK, *Raport roczny z działalności CERT Polska*, 2024, https://nask.pl [dostęp: 17.12.2025].
45. NASK, *Raport roczny z działalności*…, s. 89.
46. Orange Polska, *CyberTarcza: raport bezpieczeństwa 2024*, 2024, https://www.orange.pl/bezpieczenstwo [dostęp: 17.12.2025].

Również w Barometrze Cyberbezpieczeństwa KPMG za najgroźniejsze uznano kradzieże danych poprzez phishing, co potwierdza skalę tego zagrożenia[47].

- Ransomware: złośliwe szyfrowanie danych i żądania okupu to jeden z najbardziej destrukcyjnych rodzajów ataku. W 2024 roku CERT Polska zarejestrował 147 incydentów ransomware (8% mniej niż w roku 2023), przy czym ofiarami były głównie firmy (87 przypadków) i instytucje publiczne (25 przypadków). Ransomware zazwyczaj powoduje całkowity paraliż działania ofiary ataku (średnio ponad dwa tygodnie przestojów) i – w razie wypłaty okupu – poważne straty finansowe[48]. W pierwszej połowie 2025 roku Polska znalazła się na pierwszym miejscu na świecie pod względem liczby wykrytych ataków ransomware (6% detekcji). Co może zaskakiwać, aż 17% pracowników, którzy padli ofiarą cyberataku, nie poinformowało nikogo o takim zdarzeniu[49].
- Ataki DDoS (zakłócenie usług): choć rzadziej ujawniane w statystykach CERT Polska, to DDoS-y pozostają realnym zagrożeniem dla wielu organizacji. CERT Orange Polska w swoim raporcie wspomniał m.in. o obronie przed rekordowym atakiem w Polsce o mocy 1,3 Tbps[50]. Operatorzy cyberbezpieczeństwa implementują systemy „blokowania" masowych zgłoszeń (np. zagrożeń SMS)[51]. W 2024 roku do CERT Polska wpłynęło blisko 355 tys. zgłoszeń podejrzanych wiadomości SMS (smishing) – o 60% więcej niż rok wcześniej, z których system blokady ograniczył aż 1,5 mln złośliwych SMS-ów[52].
- Zaawansowane ataki ukierunkowane (APT): w przeglądzie incydentów CERT Polska odnotowuje działania grup APT, zwłaszcza wymierzone w sektor publiczny i strategiczny. Ze sprawozdania CSIRT Gov wynika, że w 2024 roku łącznie zarejestrowano 111 660 incydentów na poziomie krajowym (wzrost o 23% r/r), w tym 103 449 obsłużył CERT NASK. Chociaż nie wszystkie z nich to ataki APT, wzrost liczby poważnych incydentów o 57% (w tym 58% więcej w sektorze publicznym) świadczy o nasileniu skomplikowanych i celowanych ataków na administrację i kluczowe w państwie instytucje[53].
- Wyciek danych i ataki na łańcuchy dostaw: coraz istotniejsze są incydenty polegające na kradzieży wrażliwych informacji. Przykładem z Polski jest m.in. atak na jednostkę samorządu terytorialnego – powiat jędrzejowski, w wyniku którego miała miejsce kradzież danych osobowych 80 tys. mieszkańców[54]. Tak poważny wyciek stanowił jeden z największych incydentów naruszenia ochrony danych w Polsce. Z kolei na poziomie globalnym coraz więcej uwagi poświęca się zagrożeniom łańcucha dostaw (supply chain). Dla przykładu: w 2024 roku miała miejsce awaria oprogramowania CrowdStrike Falcon, która dotknęła miliony komputerów[55].

47. KPMG Polska, *Barometr cyberbezpieczeństwa*…
48. *Raport roczny z działalności CERT Polska*…, s. 16–19 [dostęp: 17.12.2025].
49. K. Sadkowski, *Polska najczęściej na świecie atakowana ransomware w 2025*, ESET, 3.09.2025, www.eset.com [dostęp: 17.12.2025].
50. K. Gwóźdź, *CERT Poland 2024 reports – what's new in cyber security?*, 23.05.2025, https://nullbytecode.com [dostęp: 17.12.2025].
51. Orange Polska, *CyberTarcza*…
52. NASK, *Raport roczny z działalności*…
53. NASK, *Raport roczny z działalności*…
54. O. Klimczuk, *Najważniejsze incydenty w 2024 roku*, 31.12.2024 r., https://cyberdefence24.pl [dostęp: 17.12.2025].
55. O. Klimczuk, *Najważniejsze incydenty*…

Choć incydenty łańcucha dostaw nie były głównym tematem polskich raportów, dyrektywa NIS2 szczególnie podkreśla potrzebę ochrony dostawców i narzędzi, z których korzystają[56].

W badaniach i raportach podkreśla się, że główne źródła podatności na zagrożenia to czynniki ludzkie, finansowe i organizacyjne, w szczególności podane poniżej.

- Niedobór ludzi i budżetu. Barometr KPMG 2024 wskazuje, że ponad połowa firm uważa, że największymi wyzwaniami w budowaniu bezpieczeństwa są trudności z rekrutacją i utrzymaniem wykwalifikowanych specjalistów z IT[57]. Blisko 25% badanych ekspertów ds. cyberbezpieczeństwa dostrzega niedofinansowanie podstawowych elementów ochrony cyfrowej, co ujawnia istotne luki w organizacjach. Oznacza to, że mimo relatywnie dobrego pokrycia kluczowych zabezpieczeń, wiele strategii bezpieczeństwa nadal pozostaje narażonych na słabe punkty, które mogą obniżać skuteczność całej ochrony[58]. Małe firmy i samorządy często nie inwestują w aktualizacje, monitoring czy też zaawansowane narzędzia[59].
- Częstotliwość szkoleń i świadomość pracowników. ESET alarmuje, że w małych firmach pracownicy rzadko biorą udział w szkoleniach, co sprawia, że lukę poznawczą łatwiej wykorzystują przestępcy i w efekcie powstają poważne w skutkach luki kompetencyjne, które drastycznie obniżają skuteczność reagowania na realne zagrożenia[60]. Pracownicy MŚP często dysponują ograniczonym zapleczem szkoleniowym – z raportu ESET wynika, że co drugi pracownik (55%) nie uczestniczył w żadnym szkoleniu z cyberbezpieczeństwa w latach, które były objęte badaniem[61]. Poziom znajomości podstawowych pojęć z zakresu cyberbezpieczeństwa wśród pracowników pozostaje wyraźnie zróżnicowany. Większość (66%) pracowników badanych przez ESET deklarowała podstawową znajomość pojęcia pishingu, co nadal należy uznać za wynik niski, biorąc pod uwagę, że jest to najczęściej wykorzystywana metoda działania cyberprzestępców. Jeszcze słabiej wypada świadomość bardziej zaawansowanych zagrożeń – bowiem jedynie 42% pracowników wie, czym jest z kolei deepfake[62].
- Przestarzałe systemy i oprogramowanie. Wiele MŚP i jednostek samorządowych nadal używa starych systemów operacyjnych lub aplikacji bez wsparcia producenta, co znacznie zwiększa ryzyko cyberataków.
- Brak formalnych procedur i analiz ryzyka. Znaczna część JST działa intuicyjnie, bez polityk bezpieczeństwa i ciągłej analizy ryzyka. Poradnik *Cyberbezpieczny samorząd* opisuje jednostki na najniższym poziomie dojrzałości, które działają *ad hoc*, bez wdrożonego systemu zarządzania bezpieczeństwem i zawężają swoje działania do podstawowych zabezpieczeń technicznych[63].

Skutki cyberataków dla obu sektorów są wielowymiarowe. Wśród konsekwencji najczęściej wymienianych przez ekspertów są: utrata danych firmowych (34%), straty finansowe (30%),

56. J. Sypniewska, *Jak NIS2 wpłynie na podejście do bezpieczeństwa łańcucha dostaw?*, 26.06.2023 r., https://www.ey.com/pl_pl/insights/law/nis2-bezpieczenstwo-lancucha-dostaw [dostęp: 17.12.2025].
57. KPMG Polska, *Barometr cyberbezpieczeństwa*…
58. KPMG Polska, *Barometr cyberbezpieczeństwa*…, s. 5–10.
59. ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*…
60. ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*…, s. 16.
61. ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*…, s. 30–35.
62. ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*…
63. Ministerstwo Cyfryzacji, *Cyberbezpieczny samorząd 2024*…

przerwy w działalności operacyjnej (28%), koszty wizerunkowe (24%) oraz kary za naruszenie przepisów (23%)[64]. Rosnąca skala zagrożeń i coraz częstsze incydenty w Polsce pokazują, że sektory MŚP i JST potrzebują nie tylko zintegrowanych działań prewencyjnych, lecz także dostępu do usług i narzędzi ograniczających konsekwencje incydentów – w tym rozwiązań oferowanych przez zakłady ubezpieczeń.

3. Zakres i charakterystyka produktów krajowych zakładów ubezpieczeń w zakresie cyberubezpieczeń w sektorze MŚP i w JST

Celem badań przedstawionych w niniejszym artykule jest analiza zakresu i charakterystyki produktów cyberubezpieczeniowych dostępnych na polskim rynku, skierowanych do sektora MŚP oraz do JST. Analiza produktów krajowych zakładów ubezpieczeń koncentruje się na zestawieniu skali zagrożeń wynikających z cyberincydentów z rzeczywistym poziomem ochrony finansowej oferowanej MŚP oraz JST. W ramach badań utworzono matrycę ryzyk oraz odpowiadających im usług z zakresu cyberubezpieczeń, co pozwoliło na ocenę adekwatności i kompletności dostępnych produktów. Sformułowane wnioski mają na celu wskazanie obszarów, w których działania regulacyjne, edukacyjne lub rozwojowe po stronie ubezpieczycieli mogłyby przyczynić się do wzrostu dostępności produktów ubezpieczeniowych obejmujących cyberzagrożenia. Badanie obejmuje również analizę ewentualnych barier podażowych wpływających na możliwości ubezpieczenia przez te podmioty. W próbie uwzględniono podmioty z Działu II rynku ubezpieczeniowego działające w formie spółki akcyjnej (22 podmioty) oraz w formie towarzystwa ubezpieczeń wzajemnych (5 podmiotów). Z analizy wyłączono podmioty w formie oddziałów zakładów ubezpieczeń państw członkowskich UE oraz państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) z uwagi na niski udział sprzedaży ubezpieczeń brutto (Dział II) w Polsce[65]. Autorzy świadomie ograniczyli zakres badania do krajowych zakładów ubezpieczeń prowadzących działalność na rynku polskim. Jego celem było bowiem uzyskanie jednorodnej próby badawczej umożliwiającej porównanie produktów podmiotów funkcjonujących w zbliżonych uwarunkowaniach regulacyjnych, organizacyjnych i rynkowych, wpływających na koszty prowadzenia biznesu i apetyt na ryzyko ubezpieczycieli, a tym samym na strukturę oferowanych przez nich usług. Analizą objęto wyłącznie dedykowane produkty cyberubezpieczeniowe (stand-alone) z klauzulami dodatkowymi, których podstawowym przedmiotem ochrony są ryzyka cybernetyczne.

Analiza została przeprowadzona według stanu formalno-prawnego oraz produktów dostępnych na dzień 31 grudnia 2025 roku. Tak sformułowany zakres pozwolił na transparentne porównanie produktów oraz analizę ich dostępności i adekwatności dla sektora publicznego oraz małych i średnich przedsiębiorstw w Polsce (tabela 1.).

64. ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*…, s. 12.

65. KNF, „Biuletyn Kwartalny. Rynek ubezpieczeń" 2025, nr 2, https://www.knf.gov.pl/podmioty/Podmioty_rynku_ubezpieczeniowego/Dzial_II_pozostale_ubezpieczenia_osobowe_i_majatkowe_Oddzialy_zagranicznych_zakladow_ubezpieczen [dostęp: 17.12.2025].

Tabela 1. Dział II – składka przypisana brutto i produkty z obszaru cyberubezpieczeń krajowych zakładów ubezpieczeń wg stanu na dzień 31 grudnia 2025 roku

Nazwa podmiotu	Składka przypisana brutto (w tys. zł)	Działalność bezpośrednia - grupy ubezpieczeń				Czy podmiot ubezpieczeniowy posiada dedykowaną ofertę cyberubezpieczenia dla MŚP oraz JST?
		9	13	16	17	
PZU SA	**12 763 699**	**x**	**x**	**x**	**x**	**tak**
TUiR WARTA S.A.	9 730 121	x	x	x	x	nie
STU ERGO HESTIA SA	**7 355 399**	**x**	**x**	**x**	**x**	**tak**
UNIQA TU S.A.	3 785 541	x	x	x	x	nie
COMPENSA TU S.A. Vienna Insurance Group	3 123 654	x	x	x	x	nie
GENERALI T.U. S.A.	**2 092 610**	**x**	**x**	**x**	**x**	**tak**
TUiR ALLIANZ POLSKA S.A.	**1 817 067**	**x**	**x**	**x**	**x**	**tak (wyłącznie dla MŚP)**
INTERRISK TU S.A. Vienna Insurance Group	1 403 031	x	x	x	x	nie
TUW PZUW	**804 587**	**x**	**x**	**x**		**tak**
LINK4 TU S.A.	775 004	x	x	x		nie
PTR S.A.	722 186					nie
TUW TUW	490 488	x	x	x	x	nie
PKO TU S.A.	445 733	x	x	x	x	nie
TUZ UBEZPIECZENIA TU S.A.	339 943	x	x	x	x	nie
AGRO UBEZPIECZENIA TUW	329 087	x	x	x		nie
TU EULER HERMES S.A.	321 848	x		x		nie
TU INTER POLSKA S.A.	189 594	x	x	x	x	nie
TU EUROPA S.A.	174 761	x	x	x	x	nie
NATIONALE-NEDERLANDEN TU S.A.	159 506	x	x	x		nie
TU ZDROWIE S.A.	149 067					nie
KUKE S.A.	135 081					nie
SIGNAL IDUNA POLSKA TU S.A.	121 405	x	x	x		nie
SANTANDER ALLIANZ TU S.A.	114 848	x	x	x		nie
SALTUS TUW	109 405	x	x	x		nie
TUW- CUPRUM	92 935	x	x			nie
CREDIT AGRICOLE TU S.A.	79 074	x	x	x		nie
PARTNER TUiR S.A.	6 665	x	x	x		nie
Razem	47 632 339	24	23	23	13	5

Źródło: opracowanie własne na podstawie: KNF, 2025, „Biuletyn Kwartalny. Rynek ubezpieczeń" 3/2025, https://www.knf.gov.pl/podmioty/Podmioty_rynku_ubezpieczeniowego/Dzial_II_pozostale_ubezpieczenia_zaklady_ubezpieczen_dzialajace_w_formie_spolki_akcyjnej [dostęp: 17.12.2025].

Analizując dane zebrane w tabeli 1., można wyciągnąć wniosek, iż umocowanie do sprzedaży ubezpieczeń z grupy 9[66] mają aż 24 zakłady ubezpieczeń. Grupy 13 (OC) oraz 16 (ryzyka finansowe)[67] są również standardem rynkowym większości ubezpieczycieli (23 podmioty). Uprawnienia w zakresie ubezpieczeń ochrony prawnej[68] ma już w swojej ofercie zdecydowanie najmniej ubezpieczycieli (13 podmiotów). Wydaje się jednak, że najbardziej pożądane przez klientów są ubezpieczenia w obszarze finansowym. Większość analizowanych podmiotów dysponuje umocowaniem na wykonywanie działalności w ramach grupy 16, co wskazuje, że ryzyka finansowe stanowią istotny element ich portfeli produktowych. Brak umocowania dotyczy nielicznych

66. Grupa 9 – ubezpieczenia pozostałych szkód rzeczowych (jeżeli nie zostały ujęte w grupach 3, 4, 5, 6 lub 7), wywołanych przez grad lub mróz oraz inne przyczyny (jak np. kradzież), jeżeli przyczyny te nie są ujęte w grupie 8.
67. Grupa 13 – ubezpieczenia odpowiedzialności cywilnej (ubezpieczenie odpowiedzialności cywilnej ogólnej) nieujętej w grupach 10–12; Grupa 16 – ubezpieczenia ryzyk finansowych, w tym: m.in. utraty zysków, stałych wydatków ogólnych, nieprzewidzianych wydatków handlowych oraz innych strat finansowych).
68. Grupa 17 – ubezpieczenia ochrony prawnej.

zakładów, zwykle mniejszych lub o wyspecjalizowanym charakterze działalności (np. TUW-Cuprum, KUKE S.A., PTR S.A.). Mimo szerokiego dostępu do grupy 16, propozycja produktów cyberubezpieczeniowych pozostaje ograniczona i słabo rozpowszechniona. Zaledwie kilka podmiotów – PZU SA, ERGO Hestia, Generali, TUW PZUW oraz Allianz – oferuje pełne cyberubezpieczenia skierowane do MŚP i do JST. W przypadku Allianz zakres produktów jest ograniczony jedynie do sektora MŚP. Zdecydowana większość zakładów, w tym duże podmioty o istotnej pozycji rynkowej (WARTA, UNIQA, Compensa, InterRisk, Nationale-Nederlanden), nie posiada dedykowanych cyberproduktów, co wskazuje na niski poziom rozwinięcia tej linii biznesowej. Brak jednoznacznej zależności między wolumenem składki a gotowością do oferowania cyberubezpieczeń. Choć część liderów rynku (PZU, ERGO Hestia, Generali) aktywnie rozwija cyberprodukty, to już inne duże zakłady – takie jak WARTA i UNIQA – pozostają nieobecne w tym segmencie. Oznacza to, że obecność w obszarze cyberubezpieczeń nie jest funkcją wyłącznie skali działalności, lecz wynika raczej z indywidualnych strategii produktowych i zarządzania ryzykiem. Towarzystwa ubezpieczeń wzajemnych (TUW) wykazują minimalną aktywność w obszarze cyber. TUW charakteryzują się z reguły niższym przypisem składki oraz bardziej tradycyjnym modelem działania, co może ograniczać ich zdolność do rozwoju innowacyjnych produktów. Jedynymi wyjątkami są TUW PZUW (oferujący cyberubezpieczenia) oraz Saltus TUW (umocowanie, lecz bez takiego produktu). Dla pozostałych TUW cyberubezpieczenia nie były na moment przeprowadzenia badania obszarem aktywności. Na tym tle wiodące towarzystwa komercyjne wykazują wyraźnie większą aktywność produktową. Istotnym problemem ograniczającym rozwój rynku cyberubezpieczeń pozostaje również ograniczona dostępność danych dotyczących szkód cybernetycznych oraz asymetria informacji pomiędzy ubezpieczycielem a ubezpieczonym. Czynniki te utrudniają prawidłową ocenę ryzyka, kalkulację składki oraz rozwój bardziej zaawansowanych produktów cyberubezpieczeniowych.

Przykładem podmiotu dominującego w zakresie cyberubezpieczeń jest największy ubezpieczyciel w Polsce czyli PZU S.A. Tabela 2. prezentuje syntetyczne zestawienie kluczowych kategorii ryzyk cybernetycznych wraz z informacją, czy są one objęte ochroną w ramach Ogólnych Warunków Ubezpieczenia od ryzyk cybernetycznych PZU S.A. Opracowanie wskazuje również zakres ochrony oraz istotne ograniczenia wynikające z definicji i konstrukcji OWU. Celem tabeli jest umożliwienie szybkiej oceny, w jakim stopniu ubezpieczenie PZU odpowiada na najczęściej występujące ryzyka cybernetyczne oraz jakie elementy mogą wymagać dodatkowej analizy lub rozszerzenia ochrony.

Tabela 2. Zakres ochrony ubezpieczeniowej ryzyk cybernetycznych w OWU PZU S.A. – stan na dzień 31 grudnia 2025 roku

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU?	Zakres ochrony / ograniczenia
Złośliwe oprogramowanie (malware, wirusy, ransomware)	Tak	Obejmuje złośliwe oprogramowanie w ramach definicji Zdarzenia Cybernetycznego; ochrona dotyczy m.in. ransomware, uszkodzenia danych oraz kosztów ich odtworzenia (pkt 2.37, 2.38).
Phishing	Częściowo	Ochrona skutków phishingu wyłącznie wtedy, gdy prowadzi do naruszenia danych lub nieuprawnionego dostępu; brak ochrony dla wyłudzeń finansowych (pkt 3.19).

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU?	Zakres ochrony / ograniczenia
Atak blokujący dostęp (DoS / DDoS)	Tak	Obejmuje zakłócenie dostępności systemu jako Zdarzenie Cybernetyczne; ochrona obejmuje skutki przerwania lub zakłócenia działalności (pkt 2.37.3).
Naruszenie bezpieczeństwa danych	Tak	Obejmuje utratę, wyciek lub naruszenie poufności danych oraz koszty powiadomień, obsługi prawnej i naprawy szkody (pkt 2.16).
Atak cybernetyczny i naruszenie prywatności (RODO)	Tak	Ochrona roszczeń osób trzecich związanych z naruszeniem danych; kary administracyjne objęte tylko w zakresie prawnie dopuszczalnym (pkt 1.1, 1.3, 2.26).

Źródło: opracowanie własne na podstawie: Ogólne warunki ubezpieczenia od ryzyk cybernetycznych ustalone uchwałą Zarządu Powszechnego Zakładu Ubezpieczeń Spółki Akcyjnej nr UZ/162 z dnia 31 maja 2023 r.

OWU PZU S.A. obejmują ochroną kluczowe kategorie ryzyk cybernetycznych. Ubezpieczenie obejmuje skutki ataków DoS/DDoS, traktowanych jako zdarzenia cybernetyczne powodujące przerwy lub zakłócenia działalności, a także naruszenia bezpieczeństwa danych, w tym utratę lub wyciek informacji oraz koszty prawne i organizacyjne związane z obsługą incydentu. Ponadto przewidziana jest ochrona odpowiedzialności cywilnej za naruszenia prywatności, przy czym kary administracyjne, w tym wynikające z RODO, objęte są wyłącznie w zakresie prawnie dopuszczalnym. Po omówieniu zakresu ochrony w ramach OWU PZU S.A. zasadnym jest przejście do kolejnego elementu analizy, obejmującego porównanie struktury i zakresu ubezpieczenia cybernetycznego oferowanego przez kolejne towarzystwo.

Informacje zawarte w tabeli 3. prezentują w sposób syntetyczny, jak ERGO Hestia S.A. definiuje i obejmuje ochroną kluczowe kategorie cyberryzyk. Zestawienie to pozwala ocenić różnice w podejściu do ochrony danych, reakcji na incydenty cybernetyczne oraz do interpretacji zdarzeń takich jak ataki złośliwego oprogramowania, phishing czy naruszenia prywatności.

Tabela 3. Zakres ochrony ubezpieczeniowej ryzyk cybernetycznych w OWU Ergo Hestia S.A. – stan na dzień 31 grudnia 2025 roku

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU?	Zakres ochrony / ograniczenia
Złośliwe oprogramowanie (malware, wirusy, ransomware)	Tak	Obejmuje złośliwe oprogramowanie w ramach definicji ataku komputerowego; ochrona obejmuje szkody w danych, koszty reagowania, odpowiedzialność cywilną oraz utratę zysku (definicja ataku komputerowego §4 ust. 3; sekcje I, II, III, IV).
Phishing	Częściowo	Ochroną objęte są jedynie skutki phishingu, jeśli doprowadził do ataku komputerowego; brak ochrony samych wyłudzeń finansowych (brak definicji phishingu; §4 ust. 3).
Atak blokujący dostęp (DoS / DDoS)	Tak	Obejmuje blokadę usług wprost jako atak komputerowy, jeśli prowadzi do zakłócenia systemów (definicja §4 ust. 2 i §4 ust. 3).
Naruszenie bezpieczeństwa danych	Tak	Ochrona obejmuje szkody w danych oraz odpowiedzialność za naruszenia danych wobec osób trzecich (sekcje I i III).

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU?	Zakres ochrony / ograniczenia
Naruszenie prywatności (RODO)	Częściowo	Ochrona roszczeń i kosztów postępowań; kary administracyjne są wyłączone, chyba że wykupiono dodatkową klauzulę (sekcje I i III; kary – klauzula 3002).

Źródło: opracowanie własne na podstawie: Ogólne warunki ubezpieczenia od ryzyk cybernetycznych Ergo Hestia S.A. nr MP/OW172/2503 z dnia 1 kwietnia 2025 r.

Z analizy tabeli 3. wynika, że OWU Ergo Hestia S.A. zapewniają szeroką ochronę w zakresie technicznych skutków cyberataków, w tym malware, ataków DoS/DDoS oraz naruszeń bezpieczeństwa danych, obejmując zarówno szkody w danych, jak i odpowiedzialność cywilną. Jednocześnie istotne ograniczenia występują w obszarze phishingu oraz naruszeń prywatności, gdzie ochrona ma charakter warunkowy lub wymaga wykupienia dodatkowych klauzul, co wskazuje na potencjalne luki w ochronie finansowej bez rozszerzeń umowy. Po przedstawieniu podejścia ERGO Hestii do podstawowych ryzyk cybernetycznych kolejnym etapem jest analiza zakresu ochrony oferowanej przez Generali. Tabela 4. przedstawia zestawienie kluczowych kategorii cyberryzyk oraz opis, w jaki sposób poszczególne zdarzenia są definiowane i objęte ochroną w ramach OWU CyberRED. Zestawienie to umożliwia ocenę kompleksowości oferowanej ochrony, identyfikację ograniczeń oraz porównanie z rozwiązaniami konkurencyjnymi na rynku.

Tabela 4. Zakres ochrony ubezpieczeniowej ryzyk cybernetycznych w OWU Generali S.A. – stan na dzień 31 grudnia 2025 roku

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU ?	Zakres ochrony / ograniczenia
Złośliwe oprogramowanie (malware, wirusy, ransomware)	Tak	Obejmuje złośliwe oprogramowanie w ramach definicji Incydentu; ochrona obejmuje reakcję, odtworzenie danych, przerwanie działalności, reputację, wymuszenie oraz cyberkradzież (sekcje 1, 2, 3, 4, 5, 6, 8, 9).
Phishing	Częściowo	Ochrona dotyczy jedynie skutków phishingu, jeśli doprowadził do incydentu, np. kradzieży danych, cyberkradzieży lub naruszenia danych osobowych; brak ochrony samych wyłudzeń finansowych (sekcje 1, 6, 8).
Atak blokujący dostęp (DoS / DDoS)	Tak	Obejmuje blokadę usług w ramach definicji Incydentu; ochrona dotyczy reakcji, naprawy, utraty zysku oraz odpowiedzialności wobec osób trzecich (sekcje 1, 2, 3, 9).
Naruszenie bezpieczeństwa danych	Tak	Ochrona obejmuje naruszenie, uszkodzenie lub kradzież danych, a także roszczenia osób trzecich z tym związane (sekcje 1, 2, 8).
Naruszenie prywatności (RODO)	Tak	Ochrona roszczeń osób trzecich oraz naruszeń prywatności w treściach internetowych; koszty postępowań administracyjnych są objęte, natomiast kary tylko jeśli dopuszcza to prawo (sekcje 1, 8, 10).

Źródło: opracowanie własne na podstawie: CyberRED – kompleksowe ubezpieczenie ryzyk związanych z naruszeniem cyberbezpieczeństwa. Ogólne Warunki Ubezpieczenia obowiązujące od 20 stycznia 2022 r.

Wyniki analizy wskazują, że OWU Generali T.U. S.A. zapewniają bardzo szeroki i kompleksowy zakres ochrony cybernetycznej, obejmujący zarówno skutki techniczne incydentów (malware, DoS/DDoS, naruszenia danych), jak i konsekwencje finansowe, reputacyjne oraz odpowiedzialność wobec osób trzecich. Ograniczenia dotyczą głównie phishingu, który objęty jest ochroną jedynie pośrednio, oraz kar administracyjnych RODO, które są objęte wyłącznie w zakresie prawnie dopuszczalnym.

Po omówieniu zakresu ochrony oferowanego przez Generali, kolejnym elementem analizy jest przedstawienie podejścia Allianz Polska S.A., którego konstrukcja OWU Cyber Protect opiera się na szerokiej definicji cyberataku oraz zestawie klauzul funkcjonalnych obejmujących zarówno szkody własne, jak i odpowiedzialność cywilną. Tabela 5. syntetyzuje sposób, w jaki Allianz klasyfikuje i obejmuje ochroną podstawowe kategorie cyberryzyk, co pozwala na bezpośrednie porównanie z innymi analizowanymi towarzystwami. Warto nadmienić, że produkt Allianz skierowany jest wyłącznie do sektora MŚP.

Tabela 5. Zakres ochrony ubezpieczeniowej ryzyk cybernetycznych w OWU Allianz Polska S.A. – stan na dzień 31 grudnia 2025 roku

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU ?	Zakres ochrony / ograniczenia
Złośliwe oprogramowanie (malware, wirusy, ransomware)	Tak	Obejmuje cyberataki polegające na instalacji złośliwego oprogramowania; ochrona obejmuje reakcję na incydent, usuwanie skutków oraz utratę zysku (na podstawie definicji Cyberataku oraz klauzul 1.1, 1.2, 1.6, 1.7, 1.8).
Phishing	Częściowo	Brak osobnej definicji; ochrona dotyczy jedynie skutków phishingu, jeśli doprowadził do cyberataku lub naruszenia danych. Brak ochrony samych wyłudzeń finansowych (zgodnie z zakresem klauzul 1.1, 1.6, 1.7).
Atak blokujący dostęp (DoS / DDoS)	Tak	Obejmuje ataki polegające na zakłócaniu działania systemów IT poprzez blokadę usług (zgodnie z definicją Cyberataku – pkt 3.2).
Naruszenie bezpieczeństwa danych	Tak	Ochrona szkód w danych, kosztów reagowania oraz odpowiedzialności wobec osób trzecich (zgodnie z klauzulami 1.1 i 1.2).
Naruszenie prywatności (RODO)	Tak	Ochrona roszczeń i kosztów postępowań administracyjnych; kary administracyjne objęte wyłącznie w granicach dopuszczalnych prawem (klauzule 1.1 oraz 1.4).

Źródło: opracowanie własne na podstawie: Ogólne warunki ubezpieczenia Technologii cyfrowych i ochrony danych, Allianz Cyber Protect, TCOD-001 02/24.

Z analizy tabeli 5. wynika, że OWU Allianz Polska S.A. zapewniają solidną ochronę podstawowych ryzyk cybernetycznych, w tym malware, ataków DoS/DDoS oraz naruszeń bezpieczeństwa danych, obejmującą zarówno reakcję na incydent, jak i skutki finansowe oraz odpowiedzialność cywilną. Jednocześnie phishing objęty jest ochroną jedynie pośrednio, a kary administracyjne RODO podlegają ochronie wyłącznie w zakresie dopuszczalnym przez obowiązujące przepisy prawa. Po analizie produktów komercyjnych towarzystw ubezpieczeniowych zasadnym jest przejście do modelu wzajemnościowego, reprezentowanego przez TUW PZUW, co pozwala ocenić, czy zakres ochrony cybernetycznej w tego typu podmiocie nie odbiega od standardów rynkowych. Wnioski z tabeli 6. wskazują, że OWU TUW PZUW oferują bardzo szeroki i spójny zakres ochrony

cybernetycznej, obejmujący wszystkie kluczowe kategorie ryzyk, w tym malware, phishing, ataki DoS/DDoS, naruszenia danych oraz prywatności. Na tle pozostałych ubezpieczycieli wyróżnia się pełnym ujęciem phishingu w definicjach OWU oraz objęciem kar administracyjnych RODO w zakresie dopuszczalnym prawem.

Tabela 6. Zakres ochrony ubezpieczeniowej ryzyk cybernetycznych w OWU TUW PZUW – stan na dzień 31 grudnia 2025 roku

Kategoria ryzyka cybernetycznego	Czy ryzyko cybernetyczne zawarte jest w treści OWU?	Zakres ochrony / ograniczenia
Złośliwe oprogramowanie (malware, wirusy, ransomware)	Tak	Obejmuje złośliwe oprogramowanie w ramach definicji Ataku Komputerowego, a także cyberwymuszenie związane z ransomware; ochrona obejmuje szkody w danych, koszty odtworzenia, utratę zysku oraz odpowiedzialność cywilną (definicje Ataku Komputerowego i Cyber Wymuszenia; Rozdział II lit. A–H).
Phishing	Tak	Ochroną objęte są skutki phishingu, który jest wprost elementem definicji Naruszenia Bezpieczeństwa Sieci Komputerowej; ochrona dotyczy naruszeń danych, nieuprawnionego dostępu lub innych cyberincydentów, lecz nie obejmuje wyłudzeń finansowych bez incydentu cyber (Rozdział VI pkt 18 ppkt 2).
Atak blokujący dostęp (DoS / DDoS)	Tak	Obejmuje blokadę usług jako Atak Komputerowy; ochrona obejmuje koszty reagowania, utratę zysku, zakłócenie usług własnych i chmurowych oraz odpowiedzialność cywilną wobec osób trzecich (definicja Ataku Komputerowego; Rozdział II lit. C–D, Rozdział III lit. M).
Naruszenie bezpieczeństwa danych	Tak	Ochrona obejmuje utratę, wyciek, modyfikację lub zniszczenie danych oraz koszty powiadomień, działania naprawcze i odpowiedzialność wobec osób trzecich (definicja Naruszenia Bezpieczeństwa Sieci Komputerowej; Rozdział II lit. A–B; Rozdział III lit. I).
Naruszenie prywatności (RODO)	Tak	Obejmuje naruszenia prywatności oraz danych osobowych, w tym roszczenia osób trzecich, koszty postępowań administracyjnych oraz kary administracyjne w zakresie dopuszczonym prawem (definicja Naruszenia Prywatności; Rozdział III lit. I–J).

Źródło: Ogólne Warunki Ubezpieczenia ryzyk cybernetycznych w TUW PZUW ustalone uchwałą Zarządu TUW PZUW nr UZ/120 z dnia 31 sierpnia 2021 r.

4. Analiza OWU – wnioski końcowe

Zakres produktowy cyberubezpieczeń dla sektora MŚP oraz dla JST jest bardzo ograniczony. Dla wielu podmiotów barierą jest wysoka niepewność i trudność w kwantyfikacji ryzyka cybernetycznego. Brak długich, jednorodnych i wystandaryzowanych szeregów danych szkodowych, szybka ewolucja zagrożeń oraz silna korelacja zdarzeń utrudniają rzetelną taryfikację składek. Problemem rynkowym są również ograniczone możliwości reasekuracyjne oraz restrykcyjne warunki oferowane przez reasekuratorów, którzy postrzegają cyberryzyko jako element ryzyka systemowego. Przekłada się to również na niższe limity odpowiedzialności, wyższe ceny ochrony reasekuracyjnej

i ostrożną politykę underwritingową ubezpieczycieli. Przeprowadzona analiza OWU wszystkich zakładów ubezpieczeń wykazała, że ochrona przed malware (w tym ransomware) oraz atakami DoS/DDoS jest standardem rynkowym, przy czym najszerszy zakres zapewnia Generali, Allianz i TUW PZUW, natomiast PZU i ERGO Hestia oferują ochronę bardziej ograniczoną. Phishing stanowi największą lukę w ochronie ubezpieczeniowej, gdyż w większości OWU chronione są jedynie jego skutki, a pełniejsze ujęcie tego ryzyka występuje wyłącznie w TUW PZUW. Naruszenia danych oraz prywatności są objęte ochroną we wszystkich analizowanych produktach, jednak różnice definicyjne i ograniczenia dotyczące kar RODO mogą istotnie wpływać na faktyczną efektywność ochrony. Na tym tle szczególnego znaczenia nabiera analiza wyłączeń odpowiedzialności zawartych w OWU, które mogą istotnie ograniczać realną skuteczność ochrony ubezpieczeniowej. Poniżej zaprezentowano pięć głównych wyłączeń odpowiedzialności, które w praktyce najsilniej ograniczają ochronę ubezpieczeniową i o których klient sektora MŚP lub JST powinien być jednoznacznie poinformowany przed zawarciem umowy. Wnioski zostały sformułowane na podstawie analizy OWU PZU, ERGO Hestia, Generali, Allianz oraz TUW PZUW.

- Brak ochrony dla „czystych" wyłudzeń finansowych. W żadnym z analizowanych OWU ochrona nie obejmuje strat finansowych wynikających wyłącznie z manipulacji socjotechnicznej, jeżeli nie doszło jednocześnie do naruszenia systemów IT lub danych. Oznacza to, że przelew wykonany „dobrowolnie" przez pracownika po phishingu lub spoofingu e-mail pozostaje poza ochroną, nawet jeśli jest to jeden z najczęstszych i najkosztowniejszych cyberincydentów.
- Wyłączenia związane z rażącym niedbalstwem i brakiem zabezpieczeń. OWU przewidują szerokie wyłączenia odpowiedzialności w przypadku braku aktualizacji systemów, niewdrożenia podstawowych zabezpieczeń, braku kopii zapasowych lub naruszenia obowiązków prewencyjnych. W praktyce oznacza to, że nawet realny cyberatak może nie zostać objęty ochroną, jeżeli ubezpieczyciel uzna, że organizacja nie dochowała „należytej staranności".
- Wyłączenie szkód istniejących lub możliwych do przewidzenia przed zawarciem umowy. OWU konsekwentnie wyłączają odpowiedzialność za incydenty, luki bezpieczeństwa lub defekty systemów istniejące przed datą retroaktywną, nawet jeśli klient nie był ich faktycznie świadomy, ale „mógł się dowiedzieć przy zachowaniu należytej staranności". To istotnie ogranicza ochronę w organizacjach o niskiej dojrzałości cyberbezpieczeństwa.
- Liczne wyłączenia kosztów pośrednich i reputacyjnych. W wielu OWU wyłączone lub silnie ograniczone są koszty pośrednie, takie jak utrata kontraktów, spadek wartości marki, utrata rynku, opóźnienia projektowe czy kary umowne wobec kontrahentów.
- Brak ochrony szkód powstałych w wyniku wojny lub operacji cybernetycznej wymierzonej przez państwo. Takie wyłączenia występują wprost w klauzulach „wojennych" oraz „terrorystycznych", które obejmują również działania w cyberprzestrzeni, nawet jeśli nie dochodzi do fizycznego konfliktu zbrojnego. Ataki typu APT, kampanie ransomware na infrastrukturę krytyczną, szpitale, JST czy sektor energetyczny są coraz częściej łączone z działaniami państwowymi lub quasi-państwowymi, co ogranicza ochronę ubezpieczeniową.

Podsumowanie

Na podstawie przeprowadzonych badań i analizy krajowej oraz zagranicznej literatury przedmiotu można wskazać trzy główne obszary działań ukierunkowanych na rozwój i rozszerzenie produktów

cyberubezpieczeniowych adresowanych do sektora MŚP i do JST. Po pierwsze, potrzebna jest większa standaryzacja definicji ryzyk cybernetycznych, zwłaszcza phishingu i cyberincydentów. Poprawiłoby to porównywalność produktów i przejrzystość ochrony. Standardy w tym zakresie mogłyby zostać zdefiniowane w nowej rekomendacji KNF, zasadach dobrych praktyk PIU lub też, co byłoby optymalnym rozwiązaniem, mogłyby mieć charakter międzysektorowy i opierać się na współpracy instytucji nadzorczych, samorządu ubezpieczeniowego oraz krajowego systemu cyberbezpieczeństwa. Po drugie, kluczowe są działania edukacyjne skierowane do klientów i pośredników, zwiększające świadomość realnych skutków cyberincydentów oraz znaczenia wyłączeń w OWU w kontekście ich pełnej ochrony. Tutaj szczególną rolę mógłby odegrać samorząd ubezpieczeniowy we współpracy z organizacjami branżowymi z zakresu cyberbezpieczeństwa. Po trzecie, po stronie ubezpieczycieli zasadne jest rozwijanie bardziej kompleksowych i elastycznych produktów, w szczególności rozszerzających ochronę przed skutkami phishingu i strat finansowych, co mogłoby istotnie zwiększyć ochronę ubezpieczeniową podmiotów.

Po stronie podaży cyberubezpieczeń dla MŚP i dla JST można wskazać kilka kluczowych barier ograniczających rozwój badanych produktów. Po pierwsze, istotną przeszkodą jest wysoka niepewność i trudność w kwantyfikacji ryzyka cybernetycznego. Brak długich, jednorodnych i wystandaryzowanych szeregów danych szkodowych, szybka ewolucja zagrożeń oraz silna korelacja zdarzeń (ryzyko kumulacji) mogą utrudniać rzetelną taryfikację składek i zarządzanie portfelem. Po drugie, problemem są ograniczone możliwości reasekuracyjne oraz restrykcyjne warunki oferowane przez reasekuratorów, którzy postrzegają cyberryzyko jako element ryzyka systemowego. Przekłada się to również na niższe limity odpowiedzialności, wyższe ceny ochrony reasekuracyjnej i ostrożną politykę underwritingową ubezpieczycieli. Po trzecie, kolejną barierę stanowią znaczne koszty operacyjne i kompetencyjne, związane z koniecznością utrzymywania wysoko wykwalifikowanych zespołów ekspertów IT, prawników oraz dostawców usług. Dla mniejszych zakładów ubezpieczeń, w tym TUW, koszty te często przewyższają potencjalne korzyści skali. Widoczna jest także ograniczona dojrzałość popytu, która pośrednio wpływa na produkty – niskie zainteresowanie ze strony MŚP i JST ogranicza opłacalność inwestycji w rozwój wyspecjalizowanych cyberproduktów. Wąska propozycja ubezpieczeniowa w obszarze cyber jest zatem efektem sprzężenia szeregu ograniczeń regulacyjnych, rynkowych i organizacyjnych, których redukcja wymaga skoordynowanych działań zarówno po stronie regulatorów, ubezpieczycieli, jak i uczestników rynku.

Przeprowadzone badania wskazują jednocześnie, że rynek cyberubezpieczeń w Polsce pozostaje na relatywnie wczesnym etapie rozwoju. Analiza produktów krajowych zakładów ubezpieczeń wykazała istnienie wyraźnej luki pomiędzy skalą i dynamiką zagrożeń cybernetycznych identyfikowanych w sektorze MŚP i oraz w JST a rzeczywistym zakresem dostępnej ochrony ubezpieczeniowej. Szczególnie widoczne jest to w odniesieniu do ryzyk związanych z phishingiem, stratami finansowymi oraz skutkami zaawansowanych incydentów cybernetycznych. Wyniki badań potwierdzają również ograniczoną dostępność dedykowanych cyberubezpieczeń dla jednostek samorządu terytorialnego oraz mniejszych podmiotów gospodarczych, które z jednej strony należą do grup najbardziej narażonych na skutki cyberataków, a z drugiej często dysponują ograniczonymi zasobami finansowymi i organizacyjnymi umożliwiającymi spełnienie wymagań stawianych przez ubezpieczycieli.

W perspektywie kolejnych lat istotny wpływ na rozwój rynku mogą wywierać europejskie regulacje dotyczące cyberbezpieczeństwa i odporności cyfrowej, w szczególności Rozporządzenie

DORA oraz Dyrektywa NIS2. Wdrażanie tych regulacji przyczynia się do upowszechniania obowiązkowych standardów cyberbezpieczeństwa, wymogów raportowania incydentów oraz systemowego zarządzania ryzykiem cyfrowym. Można oczekiwać, że proces ten będzie sprzyjał wzrostowi dojrzałości organizacyjnej przedsiębiorstw i instytucji publicznych, a tym samym stworzy warunki dla rozwoju bardziej dojrzałego, przejrzystego i porównywalnego rynku cyberubezpieczeń w Polsce. Do osiągnięcia tego celu konieczne są jednak dalsza edukacja uczestników rynku, standaryzacja definicji ryzyk i zakresów ochrony oraz pogłębienie współpracy pomiędzy sektorem publicznym, branżą ubezpieczeniową i środowiskiem cyberbezpieczeństwa. W obliczu rosnącej liczby i skali incydentów cybernetycznych, cyberubezpieczenia powinny stopniowo przestać być postrzegane wyłącznie jako fakultatywny produkt rynkowy, a stać się jednym z elementów systemowego zarządzania ryzykiem cyfrowym, uzupełniającym obowiązkowe standardy bezpieczeństwa, odporności operacyjnej i zarządzania incydentami.

Autorzy niniejszego artykułu wyrażają nadzieję, iż wskazane w jego treści wyniki badań nie tylko przyczynią się do poszerzenia wiedzy na temat cyberubezpieczeń dla MŚP i JST, ale też będą impulsem do uzupełnienia i wzbogacenia produktów niezbędnych do wzrostu cyberbezpieczeństwa w obu bardzo ważnych sektorach polskiej gospodarki. Interesującym kierunkiem dalszych badań mogłaby być analiza wpływu implementacji dyrektywy NIS2 oraz rozporządzenia DORA na rozwój rynku cyberubezpieczeń w Polsce. Zasadne wydaje się również badanie stopnia przygotowania jednostek samorządu terytorialnego oraz małych i średnich przedsiębiorstw pod kątem spełniania wymogów underwritingowych stawianych przez zakłady ubezpieczeń.

Wykaz źródeł

Biuro Bezpieczeństwa Narodowego, *Doktryna bezpieczeństwa Rzeczpospolitej Polskiej*, Warszawa 2015.

Böhme R., Kataria G., *Models and measures for correlation in cyber-insurance*, Working Paper, Workshop on the Economics of Information Security (WEIS), University of Cambridge, Cambridge 2006, http://www.econinfosec.org/archive/weis2006/docs/16.pdf [dostęp: 17.12.2025].

Business Insider, *Zarządzaj ryzykiem, nie kryzysem. Przewodnik po skutecznym cyberbezpieczeństwie dla firm*, 2024, https://businessinsider.com.pl/technologie/nowe-technologie/zarzadzaj-ryzykiem-nie-kryzysem-raport-o-cyberbezpieczenstwie-dla-firm-pobierz/4rfetwg [dostęp: 17.12.2025].

Cebula J.J., Young L.R., *A taxonomy of operational cyber security risks*, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, Pittsburgh 2010.

CERT Polska, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2024*, 2025, https://cert.pl [dostęp: 17.12.2025].

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2025, nr 1(13).

Check Point Research, *Cyber Security Report Poland 2024*, 2024, https://www.checkpoint.com [dostęp: 17.12.2025].

Chochowski K., *Strategia cyberbezpieczeństwa jako przejaw polityki administracyjnej*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Seria Prawnicza" 2019, z. 107.

CSFI, *Insurance banana skins 2023. The CSFI survey on the risk facing insurers*, 2023, The Centre for the Study of Financial Innovation, https://www.pwc.co.uk/insurance/assets/pdf/insurance--banana-skins-2023.pdf [dostęp: 17.12.2025].

Cyber resilience: The cyber risk challenge and the role of insurance, Chief Risk Officers – CRO Forum, Amsterdam, www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf, [za:] *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris 2017.

CyberRED – kompleksowe ubezpieczenie ryzyk związanych z naruszeniem cyberbezpieczeństwa. Ogólne Warunki Ubezpieczenia obowiązujące od 20 stycznia 2022 r.

EIOPA, *Cyber risk for insurers – challenges and opportunities*, European Insurance and Occupational Health Pension Authority, 2019, https://www.eiopa.europa.eu/document/download/61701869-eab9–49c7-a9ec-14d0b810f755_en?filename=Cyber%20Risk%20for%20Insurers%20-%20Challenges%20and%20Opportunities [dostęp: 17.12.2025].

ENISA, *Threat Landscape 2024 (Poland section)*, 2024, https://www.enisa.europa.eu/topics/threat--landscape [dostęp: 17.12.2025].

ESET Cybersecurity Process Protected, *Cyberportret polskiego biznesu 2025*, 2025, https://in.eset.pl/ [dostęp: 17.12.2025].

Fortinet, *Global Threat Landscape Report 2025 (Poland Highlights)*, 2025, https://www.fortinet.com [dostęp: 17.12.2025].

Gwóźdź K., *CERT Poland 2024 reports – what's new in cyber security?*, 23.05.2025 r., https://nullbytecode.com [dostęp: 17.12.2025].

ISO/IEC, *ISO/IEC 27032:2023 Information security, cybersecurity and privacy protection — Guidelines for cybersecurity*, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), Geneva 2023.

Klimczuk O., *Najważniejsze incydenty w 2024 roku*, 31.12.2024 r., https://cyberdefence24.pl [dostęp: 17.12.2025].

KNF, „Biuletyn Kwartalny. Rynek ubezpieczeń" 2025, nr 2, https://www.knf.gov.pl/?articleId=95005&p_id=18/ [dostęp: 17.12.2025].

KNF, „Biuletyn Kwartalny. Rynek ubezpieczeń" 2025, nr 3, https://www.knf.gov.pl/?articleId=96471&p_id=18 [dostęp: 17.12.2025].

KNF, Komunikaty https://www.knf.gov.pl/?articleId=91751&p_id=18, https://www.knf.gov.pl/?articleId=92241&p_id=18 [dostęp: 17.12.2025].

KPMG Polska, *Barometr cyberbezpieczeństwa 2024*, 2024, https://kpmg.com/pl [dostęp: 17.12.2025].

Małek A., Monkiewicz J., Monkiewicz M., *Ubezpieczenia w świecie cyfrowym: nowe uwarunkowania i wyzwania*, [w:], *Ubezpieczenia cyfrowe: możliwości, oczekiwania, wyzwania*, Monkiewicz J., Gąsiorkiewicz L., Gołąb P., Monkiewicz M. [red.], PWN, Warszawa 2022.

Malinowska K., *Aspekty prawne ubezpieczenia cyber ryzyk*, „Prawo Asekuracyjne" 2018, nr 2(95).

Ministerstwo Cyfryzacji, *Cyberbezpieczny samorząd 2024*, 2024, https://www.gov.pl/cyfryzacja [dostęp: 17.12.2025].

Ministerstwo Cyfryzacji, *Cyberbezpieczny samorząd 2024*, 2024, https://www.gov.pl/cyfryzacja [dostęp: 17.12.2025].

Monkiewicz J., Monkiewicz M., *Ubezpieczenia w świecie cyfrowym: nowe wyzwania*, [w:] Monkiewicz J., Gąsiorkiewicz L., *Finanse cyfrowe. Perspektywa rynkowa*, Wydawnictwo Politechniki Warszawskiej, Warszawa 2021.

Moorcraft B., *CNA concludes investigation into cyberattack*, "Insurance Business" 2021, https://www.insurancebusinessmag.com/ca/news/cyber/cna-concludes-investigation-into-cyberattack-260688.aspx [dostęp: 17.12.2025].

Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A., Sadhukhan S., *Cyber-risk decision models: To insure IT or not?*, "Decision Support Systems" 4/2013, http://dx.doi.org/10.1016/j.dss.2013.04.004.

NASK, *Raport roczny z działalności CERT Polska*, 2024, https://nask.pl [dostęp: 17.12.2025].

National Association of Insurance Commissioners – NAIC, *Cybersecurity*, USA, 2016, [za:] Strupczewski G., *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie*, „Finanse. Czasopismo Komitetu Nauk o Finansach PAN" 2017, nr 1(10).

Ogólne warunki ubezpieczenia od ryzyk cybernetycznych Ergo Hestia S.A. nr MP/OW172/2503 z dnia 1 kwietnia 2025 r.

Ogólne warunki ubezpieczenia od ryzyk cybernetycznych ustalone uchwałą Zarządu Powszechnego Zakładu Ubezpieczeń Spółki Akcyjnej nr UZ/162 z dnia 31 maja 2023 r.

Ogólne Warunki Ubezpieczenia ryzyk cybernetycznych w TUW PZUW ustalone uchwałą Zarządu TUW PZUW nr UZ/120 z dnia 31 sierpnia 2021 r.

Ogólne warunki ubezpieczenia Technologii cyfrowych i ochrony danych, Allianz Cyber Protect, TCOD-001 02/24.

Ögűt H., Raghunathan S., Menon N., *Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection*, "Risk Analysis" 2011, No. 31(3), doi: 10.1111/j.1539-6924.2010.01478.x.

Orange Polska, *CyberTarcza: raport bezpieczeństwa 2024*, 2024, https://www.orange.pl/bezpieczenstwo [dostęp: 17.12.2025].

Podlewski J., *Wdrażanie koncepcji sztucznej inteligencji w polskiej gospodarce. Problemy i rozwiązania*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2021.

PwC, *Global Digital Trust Insights 2026*, 2026, www.pwc.com [dostęp: 17.12.2025].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Rozporządzenie DORA).

Sadkowski K., *Polska najczęściej na świecie atakowana ransomware w 2025*, ESET, 3.09.2025 r., www.eset.com [dostęp: 17.12.2025].

Sypniewska J., *Jak NIS2 wpłynie na podejście do bezpieczeństwa łańcucha dostaw?*, 26.06.2023 r., https://www.ey.com/pl_pl/insights/law/nis2-bezpieczenstwo-lancucha-dostaw [dostęp: 17.12.2025].

Ten Key Questions on Cyber Risk and Cyber Risk Insurance, The Geneva Association, Zurich 2016, [za:] *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris 2017.

UK cyber security. The role of insurance in managing and mitigating the risk, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/ file/415354/UK_Cyber_Security_Report_Final.pdf [dostęp: 17.12.2025].

Vecto, *Cyberbezpieczeństwo w polskich firmach. Raport 2020*, 2020, https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2020.pdf [dostęp: 17.12.2025].

Analysis of domestic insurance companies' products in the face of growing cyber threats in small and medium-sized enterprises and local government sectors

Cyberthreats are now one of the most serious challenges for small and medium-sized enterprises (SMEs) and local government units (LGUs) in Poland. The lack of extensive IT departments, limited financial resources, and low awareness of information security often make these entities easy targets for cybercriminals. The SME and LGU sectors in Poland operate in an environment where the number and complexity of cyber threats are growing faster than the ability to neutralize them. Insurance companies offer products designed to protect customers against the negative effects of breaches of critical digital infrastructure (so-called cyberinsurance). The purpose of this article is to assess the adequacy of cybersecurity insurance offerings available on the Polish market for the SME sector and local government units by identifying the scope of coverage offered by domestic insurance companies and comparing it with the nature and scale of contemporary cyber threats. An additional objective is to identify limitations in the supply of cybersecurity products and to highlight areas requiring further market development. The article contains three substantive chapters. The first chapter discusses the theoretical foundations of cybersecurity and cyberthreats. Key cyber threats are described in the second chapter, which, like the first, is based on an analysis of domestic and international literature on the subject. Chapter three contains an empirical analysis of domestic insurance companies' (joint-stock companies and mutual insurance companies) cyber insurance offerings in the SME and local government sectors. The research findings indicate a limited number of dedicated cyber insurance products, significant variations in coverage, and a lack of full alignment between the offers and the threat structure identified in both sectors. The conclusions from the analysis can serve as a basis for further regulatory, educational, and development activities in the area of cyber insurance in Poland.

Keywords: insurance companies, SMEs, local government units, cybersecurity, cyber risk, insurance services

DR SŁAWOMIR KUJAWA – Uniwersytet Gdański Wydział Zarządzania, Katedra Bankowości i Finansów
ORCID: 0000-0001-9607-2743
e-mail: slawomir.kujawa@ug.edu.pl

DR PIOTR PISAREWICZ – Uniwersytet Gdański Wydział Zarządzania, Katedra Bankowości i Finansów
ORCID: 0000-0003-1983-1499
e-mail: piotr.pisarewicz@ug.edu.pl