dr Lyubov Klapkiv*

ZAKRES RYZYKA I SZKÓD W CYBERUBEZPIECZENIU DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

1. Wprowadzenie

Przedsiębiorstwa w Polsce przetwarzają w ramach swojej działalności coraz większe zbiory danych. Tendencja ta nasiliła się w czasie pandemii, ponieważ więcej operacji zostało przeniesiono do sieci komputerowych oraz przestrzeni wirtualnej. Zmiany technologiczne przyczyniły się do zwiększenia potencjału rozwojowego firm, ale jednocześnie podniosły też poziom zagrożeń cybernetycznych. Według raportu IBM „2021 Cost of Data Breach Report", średni całkowity koszt naruszenia ochrony danych dla organizacji wzrósł z 3,86 mln USD w roku 2020 do 4,24 mln USD w roku 2021, co stanowi najwyższy średni koszt całkowity w 17-letniej historii tego raportu [1]. Średnia wysokość okupu (*ransom*) wzrosła o 82% w latach 2020-2021. W połowie 2021 roku liczba ataków *ransomware* wzrosła o ponad 150 procent w porównaniu z całym rokiem 2020[2].

Duże przedsiębiorstwa mają większe możliwości finansowe na wyposażenie swojej działalności w wysoko zaawansowane systemy zabezpieczenia technologicznego w celu zabezpieczenia się przed takimi szkodami, natomiast średnie i małe przedsiębiorstwa nie zawsze mają wystarczające środki, żeby sfinansować zakup właściwego oprogramowania. Jednym z rozwiązań problemu zarządzania ryzykiem cybernetycznym jest jego ubezpieczenie w zakładzie ubezpieczeń.

---

* Dr Lyubov Klapkiv, Uniwersytet Marii Curie-Skłodowskiej w Lublinie.

[1] *Cost of Data Breach Report 2021*, IBM Security &Ponemon Institute, https://www.ibm.com/security/data-breach (dostęp: 14.02.2022 r.).

[2] T. Johansmeyer, *The cyber insurance market needs more money*, March 10, 2022, Harvard Business Review, https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money (dostęp: 14.02.2022 r.).

W środowisku naukowym z zakresu finansów i ekonomii temat ryzyka cybernetycznego nie jest zbyt powszechnie podejmowany. Warto jednak wymienić opracowania Boyera[3], Kshetriego[4], Romanowskego i innych[5], Strupczewskiego[6].

Rozwój cyberubezpieczeń jest dość utrudniony z uwagi na specyfikę ryzyka cybernetycznego. Można wymienić szereg czynników, które ograniczają ten proces[7]:

- brak danych historycznych, co utrudnia modelowanie predykcyjne, mogące pomóc ocenić prawdopodobieństwo straty; brak jest również kompleksowego, scentralizowanego źródła informacji o zdarzeniach cybernetycznych, z którego mogliby korzystać ubezpieczyciele, natomiast „(…) wiele, czy nawet większość zdarzeń cybernetycznych nie zostaje zgłoszona i zbadana" [8];
- większość zgłoszonych szkód dotyczy naruszenia informacji osobistych, natomiast zagrożenia typu *denial of service*, *ransomware* czy kradzież własności intelektualnej pozostają niewykryte;
- ryzyka cybernetyczne dynamicznie się zmieniają, nie są to ryzyka o charakterze stałym i standardowym. Ten fakt ogranicza wartość doświadczeń historycznych pozyskanych przez zakłady ubezpieczeń i podważa przewidywalność ekspozycji na ryzyko;
- wysokie ryzyko kumulacji szkód, co hamuje podaż na usługi reasekuracyjne w zakresie ryzyka cybernetycznego.

Cyberubezpieczenia mają dość skomplikowaną ścieżkę ewolucji. Głównym pytaniem postawionym w artykule jest kwestia tego, jakie cyberzagrożenia można ubezpieczyć w działalności małych i średnich przedsiębiorstw. Teza badawcza została sformułowana w sposób następujący: „Ubezpieczenia cybernetyczne w Polsce obejmują szeroki zakres ryzyka i szkód pochodzenia cybernetycznego co umożliwia skuteczne zarządzanie cyberryzykiem w działalności

[3] M. Boyer, *Cyber insurance demand, supply, contracts and cases*, „The Geneva Papers on Risk and Insurance – Issues and Practice", 2020, vol. 45.
[4] N. Kshetri, *The evolution of cyber-insurance industry and marke: An institutional analysis*, „Telecommunications Policy" September 2020, vol. 44, iss. 8.
[5] S. Romanosky, L. Ablon, A. Kuehn, T. Jones, *Content analysis of cyber insurance policies: how do carriers prices cyber risk*?, „Journal od Cybersecurity", 2019, vol. 5, iss. 1.
[6] G. Strupczewski, *Defining cyber risk*, „Safety science", 2021, nr 135, pp. 105-143.
[7] Deloitte Center for Financial Services, *Demystifing cyber insurance coverage report*, 2017, https://www2.deloitte.com (dostęp: 14.02.2022 r.).
[8] R. P. Hartwig, C. Wilkinson, *Cyber risks: The growing threat*, Insurance Information Institute, June 2014, p. 11. http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf. (dostęp: 14.02.2022 r.).

przedsiębiorstw". Celem artykułu jest przedstawienie aktualnego zakresu cyberryzyka oraz szkód nim wywołanych, które mogą być objęte ochroną ubezpieczeniową w praktyce ubezpieczycieli działających w Polsce.

2. Istota cyberzagrożenia

Natura zjawiska o charakterze zagrożenia w sensie ogólnym jest zawsze związana z dwoma ważnymi pojęciami – „prawdopodobieństwem" oraz „szkodą". Zagrożenie w ujęciu ekonomicznym oznacza możliwość wystąpienia zdarzenia, które prowadzi do szkody, straty lub uszkodzenia. To negatywne lub niekorzystne zdarzenie może być spowodowane działaniem podmiotu albo brakiem działania. W środowiskach innych niż cybernetyczne, zagrożenie może być spowodowane przez człowieka (*human-made*) lub być konsekwencją działania czynników przyrodniczych (np. żywioły, takie jak trzęsienie ziemi, tornado, powódź itp.).

Na czym polega specyfika zagrożenia, z jakim spotyka się przedsiębiorstwo w środowisku cybernetycznym? Wśród ekspertów nie ma zgody co do jednolitej definicji cyberzagrożeń. Słownik *Oxford English Dictionary* podaje ogólne wyjaśnienie znaczenia tego terminu jako „możliwość wystąpienia złośliwej próby uszkodzenia lub zakłócenia pracy sieci lub systemu komputerowego"[9]. Definicja ta jest dość przestarzała i niekompletna, a mimo to pomocna w zrozumieniu zjawiska cyberzagrożenia. Pierwsza część definicji podkreśla, że zagrożenie jest związane z możliwością („*possibility*") i szkodą („*damage*"). Jednak druga część, która mówi, że szkoda odnosi się do „sieci lub systemu komputerowego", nie odzwierciedla rzeczywistości. Współczesne negatywne skutki złośliwych działań w cyberprzestrzeni mogą wpływać na całościowy stan przedsiębiorstwa, jego rentowność i możliwość istnienia (szkoda wyrządzona interesom właścicieli), bezpieczeństwo narodowe i międzynarodowe (szkoda wyrządzona interesom rządu), a nawet łamać kodeks etyczny i moralny (krzywdy moralne), nie tylko w przestrzeni wirtualnej, ale także w „świecie fizycznym"[10,11]. Dlatego mówiąc o cyberzagrożeniach musimy brać pod uwagę szereg bardzo złożonych zjawisk, które wiążą się z wykorzystaniem niepodłączonych urządzeń komputerowych, danych, technologii podłączonych do Internetu *(information and communication*

[9] Definicja pojęcia „cyberzagrożenie": "the possibility of a malicious attempt to damage or disrupt a computer network or system", https://en.oxforddictionaries.com/definition/cyberthreat (dostęp: 10.04.2022 r.)

[10] S. W. Brenner, *History of computer crime*, [w:] *The history of information security*, red. K.de Leeuw, J. Bergstra, Wydawnictwo Elsevier, Amsterdam 2007.

[11] L. DeNardis, *A history of internet security*. [w:] *The history of information security*, red. K.de Leeuw, J. Bergstra, Wydawnictwo Elsevier, Amsterdam 2007.

technologies) oraz sieci komputerowych w celu wyrządzenia szkód w wymiarze cybernetycznym lub fizycznym.

Mimo że w ostatnich latach powstało wiele opracowań na temat cyberzagrożeń, w których autorzy proponują różne podejścia do typologii tego pojęcia, do dzisiaj nie powstała jednolita klasyfikacja. W opracowaniu przedstawiamy typologię cyberzagrożeń najbardziej istotnych dla środowiska przedsiębiorców. Należy jednak pamiętać, że ze względu na szybki rozwój technologii, codziennie pojawiają się nowe zagrożenia, co z kolei wyklucza stałość typologii.

W odniesieniu do każdej działalności gospodarczej zagrożenia związane z bezpieczeństwem cybernetycznym można zasadniczo podzielić na dwie kategorie. Po pierwsze, są to zagrożenia wynikające z prostych błędów technicznych, takich jak awarie systemu, w przypadku których w systemach komputerowych mogą wystąpić nieoczekiwane, niezamierzone i niezłośliwe zdarzenia, które w rezultacie mogą wpłynąć na działalność biznesową, powodując szkody. Usterki te mogą być spowodowane awarią technologii, błędem lub zaniedbaniem człowieka, bądź brakiem procedur organizacyjnych. Druga kategoria obejmuje zagrożenia związane ze złośliwymi próbami infiltracji systemów komputerowych przedsiębiorstwa przez inne osoby lub organizacje (nazywane hakerami) i spowodowania szkód finansowych lub niepieniężnych (np. utraty reputacji).

Według Pogrebnej i Skiltona, cyberzagrożenia obejmują trzy szerokie kategorie potencjalnych zagrożeń (Tab. 1)[12].

W skali światowej, obecnie największy wzrost naruszeń danych obserwuje się w sektorze ochrony zdrowia (o 55% wzrost w roku 2020 w porównaniu do roku poprzedniego[13]), co jest związane z tym, że taki zbiór danych mieści więcej wrażliwych informacji personalnych (*personally identifiable information*) niż inne sektory.

[12] G. Pogrebna, M. Skilton, *Cybersecurity Threats: Past and Present*, [w:] Navigating New Cyber Risks, red. G. Pogrebna, M. Skilton, Palgrave Macmillan, Cham 2019, p. 17.
[13] *Report on the Cybersecurity Insurance Market* – NAIC, https://content.naic.org › sites › default › files (dostęp: 10.04.2022 r.)

Tabela 1. Typologia cyberzagrożeń

Typ	Objaśnienie i przykład
Monomery	Monomery to podstawowe zagrożenia, które mogą wyrządzać szkody samodzielnie lub, co zdarza się częściej, mogą być łączone w polimery i działać jako część bardziej złożonej struktury zagrożenia. Monomery mogą występować w dwóch odmianach: podstawowej i złośliwej. Różnica między nimi polega na tym, że monomery podstawowe mogą być łagodne lub złośliwe, w zależności od sposobu ich zastosowania, natomiast złośliwe mają na celu wyrządzanie szkód. Do podstawowych monomerów należą na przykład pliki wykonywalne i *exploity*, które w zasadzie mogą być całkowicie nieszkodliwe lub mogą być zaprojektowane do wyrządzania poważnych szkód. Natomiast złośliwe monomery powodują szkodę „z założenia".
Polimery	Zagrożenia polimerowe to bardziej złożone zagrożenia, które zazwyczaj składają się z kilku monomerów. W zależności od sposobu, w jaki polimery infiltrują i atakują systemy, można je podzielić na cztery odmiany: polimery złośliwego oprogramowania, polimery techniczne o charakterze ukrytym, polimery poczty elektronicznej lub komunikatorów oraz polimery hybrydowe. Polimery złośliwego oprogramowania odnoszą się do różnych rodzajów złośliwego oprogramowania (*malware*) i obejmują wirusy (złośliwe oprogramowanie aktywowane przez użytkownika), robaki (*bugs*) (samonapędzające się złośliwe oprogramowanie) itd. Ukryte techniczne polimery reprezentują zagrożenia wykorzystujące różne środki techniczne i obejmują ataki typu *denial-of-service* (DoS, złośliwe próby spowodowania, aby ofiara, witryna lub węzeł odmówiły świadczenia usług swoim klientom), *brute force* (metoda prób i błędów stosowana do odszyfrowania zaszyfrowanych danych), itp. Polimery poczty elektronicznej i wiadomości, takie jak *phishing* (nieukierunkowane wiadomości mające na celu nakłonienie użytkowników do ujawnienia cennych informacji lub podjęcia działań korzystnych dla inicjatora cyberzagrożeń), rozprzestrzeniają się za pośrednictwem komunikacji elektronicznej.
Kompozyty	Polimery zwykle łączą się w kompozyty. Monomery mogą być integralnymi częściami takich polimerów, jak wirus lub robak, a część którą się pobiera (*payload*) jest kompozytem, który może zawierać wirusy i robaki. Z kolei pobrany plik użyteczny może być częścią złożonego kompozytu, takiego jak kradzież (cybernetyczna).

Źródło: opracowanie na podstawie: G. Pogrebna, M. Skilton, *Cybersecurity Threats: Past and Present*, [w:] Navigating New Cyber Risks, red. G. Pogrebna, M. Skilton, Palgrave Macmillan, Cham 2019, p. 17.

Pojęcie złośliwego oprogramowania (*malware*) oznacza wszelkie kody stworzone w celu:

1) usunięcia danych, zablokowania dostępu do danych lub uszkodzenia danych, z wykorzystaniem m.in. oprogramowania typu *ransomware*;

2) zniszczenia lub zakłócenia działania sieci informatycznej lub systemu komputerowego;

3) „obejścia" produktu lub usługi zapewniających bezpieczeństwo sieci informatycznej.

W literaturze poświęconej bezpieczeństwu cybernetycznemu takie zagrożenia są często związane z działalnością przestępczą w cyberprzestrzeni.

3. Ryzyko cybernetyczne jako ryzyko ubezpieczeniowe

Charakteryzując ryzyko cybernetyczne warto odnieść się do pojęć cyberzagrożenia i podatności przedsiębiorstwa na cyberzagrożenia. Podatność na ataki cybernetyczne to obiektywnie określone prawdopodobieństwo z jakim system bezpieczeństwa przedsiębiorstwa może zostać zagrożony. Innymi słowy, jest to prawdopodobieństwo, że w konkretnym systemie bezpieczeństwa istnieje luka, która może zostać wykorzystana. Ryzyko cybernetyczne jest zatem dokładnym prawdopodobieństwem, że cyberzagrożenie i podatność na ataki cybernetyczne wystąpią równocześnie w określonym miejscu i czasie, powodując szkodę.

Refsdal, Solhaud i Stolen twierdzą, że ryzyko cybernetyczne nie jest tożsame z każdym ryzykiem, na jakie może być narażony system cybernetyczny; ryzyko cybernetyczne ogranicza się do ryzyka spowodowanego przez cyberzagrożenia[14]. Ryzyko uszkodzenia serwera, na którym działa system informatyczny, na przykład w wyniku zalania wodą, nie jest ryzykiem związanym z cyberprzestrzenią, chyba że czynnikiem sprzyjającym jest cyberzagrożenie; naruszenia poufności spowodowane atakami wirusów poprzez cyberprzestrzeń oraz utrata dostępności spowodowana atakami „odmowa dostępu" (*denial of service* – DoS) są jednak przykładami zagrożeń cybernetycznych.

Ryzyko cybernetyczne przedsiębiorstwa zależy od różnych czynników wewnętrznych i zewnętrznych, w tym od wielkości aktywów firmy, wykorzystywanej przez nią technologii i jej podatności na zagrożenia, świadomości i kompetencji pracowników w zakresie bezpieczeństwa, procedur istotnych dla bezpieczeństwa cybernetycznego, bezpieczeństwa dostawców (*outsoursingu*), podatności ogólnej infrastruktury, na której opiera się działalność przedsiębiorstwa, oraz motywacji potencjalnych przestępców. Biorąc pod uwagę wszystkie

[14] A. Refsdal, B. Solhaug, K. Stølen, *Cyber-risk Management*, Springer Briefs in Computer Science. Springer, Cham 2015.

te czynniki oraz ograniczoną wiedzę na temat wpływu poszczególnych czynników na ogólne ryzyko przedsiębiorstwa, zrozumienie i oszacowanie cyberryzyka ubezpieczeniowego jest bardzo skomplikowane. Proste mierniki, takie jak liczba utraconych rekordów, nie zawsze korelują z całkowitym kosztem ryzyka[15].

W praktyce zakładów ubezpieczeń w Polsce „ryzyko cybernetyczne" jest powszechnie używane w nazwach produktów ubezpieczeniowych, natomiast ogólne warunki ubezpieczeń często obejmują również inne pojęcia, jak na przykład „zdarzenie cybernetyczne", „cyberatak", „incydent", „cyberkradzież" (Tab. 2).

Tabela 2. Zakres ryzyka cybernetycznego

ZU	Zakres ryzyka cybernetycznego	Produkt
PZU S.A.	Zdarzenie cybernetyczne: 1) użycie systemu komputerowego lub infrastruktury sieci informatycznej przedsiębiorstwa przez nieuprawnioną osobę; 2) przypadkowe usunięcie, zniszczenie lub modyfikacja danych lub oprogramowania przedsiębiorstwa przez pracownika lub dostawcę usług w chmurze; 3) atak poprzez „odmowę dostępu" (denial of service); 4) wprowadzenie złośliwego oprogramowania do jakiejkolwiek sieci należącej do lub zarządzanej przez przedsiębiorstwo, w tym sieci informatycznej któregokolwiek z dostawców usług w chmurze.	Ubezpieczenie od ryzyk cybernetycznych i związanych z RODO
Allianz S.A.	1) ukierunkowane wtargnięcie osób trzecich, które ma na celu zmodyfikowanie, zmianę, uszkodzenie, zniszczenie, usunięcie, nagranie, lub przekazanie informacji bez upoważnienia, w tym również przeniesienie danych samopowielających lub samorozprzestrzeniających się, bądź przeznaczonych do zainfekowania innych programów komputerowych, lub poprawnych danych komputerowych, uszkodzenia zasobów komputera czy innego rodzaju zakłócenia poprawnego działania systemu komputerowego; 2) działanie w celu uzyskania nieuprawnionego dostępu lub wykorzystania systemu komputerowego spółki.	Technologii cyfrowych i ochrony danych Allianz cyber protect

[15] NetDilgence: *Netdiligence cyber claims study 2014*. Technical report, NetDilligence (2014), https://www.netdiligence.com (dostęp: 10.04.2022 r.)

Tab. 2. Zakres ryzyka cybernetycznego (ciąg dalszy)

ZU	Zakres ryzyka cybernetycznego	Produkt
ERGO Hestia S.A.	1) nielegalne działania związane z uzyskaniem nieautoryzowanego dostępu do danych elektronicznych przez nieuprawnione osoby, w tym rozproszony atak dystrybucyjny DDoS lub działanie złośliwego oprogramowania. Przez nieuprawnione osoby rozumie się osoby trzecie pozostające poza stosunkiem ubezpieczenia oraz pracowników ubezpieczonego, którzy złamali zabezpieczenia lub w inny sposób zdobyli dostęp do danych elektronicznych, do których nie posiadali dostępu nadanego przez ubezpieczonego.	Ubezpieczenie od ryzyk cybernetycznych „Cyber M"
Generali Polska TU S.A.	1) bezprawny czyn lub zaniechanie zmierzające do wyrządzenia szkody lub uzyskania nielegalnego dostępu do danych, systemów teleinformatycznych lub sieci komputerowych poprzez użycie dowolnego systemu teleinformatycznego lub sieci komputerowej; 2) jakikolwiek podjęty w złym zamiarze atak skutkujący całkowitym lub częściowym ograniczeniem, zakłóceniem lub utratą dostępu do systemów teleinformatycznych i urządzeń sieciowych poprzez ich przeciążenie przychodzącym strumieniem żądań (*denial-of-service attack*), także wtedy gdy atak ma charakter rozproszony (*distributed denial-of-service attack*), 3) każdy błąd ludzki – niezamierzony lub wynikający z niedbalstwa – w zakresie wykorzystania technologii informatycznej.	CyberRED

Źródło: opracowanie własne na podstawie: https://www.pzu.pl/_fileserver/item/1515773; https://www.allianz.pl/content/dam/onemarketing/cee/azpl/dokumenty/dla-firm/ryzyka-finansowe/cyber/CYBER_owu.pdf; https://cyberochrona.ergohestia.pl/cyber-m/, https://www.generali.pl/dla-firmy/majatek/duze-przedsiebiorstwa (dostęp: 10.04.2022 r.)

Wśród najczęściej spotykanych czynów, które zostają objęte ubezpieczeniem cybernetycznych warto wymienić:

1. Naruszenie bezpieczeństwa sieci (błąd, zaniedbanie, blokada usług), na skutek którego doszło do ataku na systemy informacyjnych technologii.
2. Naruszenie danych (lub prywatności) – bezprawny dostęp, nielegalne kopiowanie, przypadkowe lub powstające w wyniku zaniedbania ujawnienie informacji o kontrahencie przedsiębiorstwa oraz jej nieuprawnione wykorzystanie przez osoby uprawnione.
3. Nieprawidłowe zachowanie związane z działalnością medialną:
   - zniesławienie, nieumyślne naruszenie własności intelektualnej, sprzeniewierzenie lub kradzież pomysłu, znaków towarowych, nazw handlowych,

szat graficznych, znaków usługowych, nazw domen, usług; kradzież informacji bądź nieuprawnione tworzenie łączy do strony docelowej;
– zakłócenie, naruszenie lub ingerencja w prawa jednostki do prywatności i wypowiedzi, ujawnienie informacji poufnych z życia prywatnego będące skutkiem rozpowszechniania tekstu, obrazu, filmu lub dźwięku za pośrednictwem witryny, obecności w mediach społecznościowych lub poczty e-mail Ubezpieczonego oraz komercyjne przywłaszczenie imienia, nazwiska, osobowości lub wizerunku.

4. Cyberatak – ukierunkowane włamanie osób trzecich do systemu komputerowego przedsiębiorstwa, które skutkuje nielegalnym i nieuprawnionym usunięciem lub zmianą danych zawartych w systemie komputerowym.
5. Cyberkradzież – nieautoryzowany elektroniczny przelew z rachunku bankowego ubezpieczonego, z brakiem możliwości jej odzyskania.

Do instrumentów, które wywołują zdarzenia ubezpieczeniowe należą:
1) złośliwe oprogramowanie (*malware*) – wrogie lub inwazyjne oprogramowanie lub kody, w tym
- wirusy komputerowe – złośliwe programy lub kody, które zagrażają programom lub plikom, nielegalnie tworząc kopię dokumentu;
- *randsomware* – programy do wymuszania okupu, szyfrując dane w komputerze, dyskach sieciowych lub danych w chmurze;

2) *phishing* – wyłudzanie od ofiary danych firmy (hasło, login, itp.);
3) atak „odmowa dostępu" (DoS) i „rozproszona odmowa dostępu" (DDOs) – zablokowanie systemu komputerowego lub usługi sieciowej z wielu źródeł w celu uniemożliwienia wykorzystania wolnych zasobów firmy.

4. Zakres szkód w ubezpieczeniu cyberryzyka przedsiębiorstw

W Polsce usługa ubezpieczenia cybernetycznego jest oferowana przez nieliczne zakłady ubezpieczeń. Niektóre z nich precyzują produkt cyberubezpieczenia dla podmiotów gospodarczych o rocznym obrocie nie przekraczającym 15 mln zł (małe i średnie firmy), a dla większych podmiotów tworzone są odrębne warunki ubezpieczenia (na przykład w ERGO Hestia są to „Cyber M" i Cyber XL"). Do grona odbiorców tej usługi wśród średnich i małych przedsiębiorstw należą sklepy internetowe (*e-commerce*), firmy produkcyjne i handlowe, firmy transportowe i budowlane, zakłady gastronomii i hotelarstwa, pośrednicy finansowi, podmioty sektora edukacji oraz ochrony zdrowia, kancelarie prawne i administracja publiczna.

W literaturze naukowej cyberubezpieczenie definiuje się jako „przeniesienie ryzyka finansowego związanego z incydentami sieciowymi i komputerowymi na

stronę trzecią”[16]. Ubezpieczenie to może przybierać różne formy, oferując ubezpieczenie odpowiedzialności cywilnej oraz obejmując różne rodzaje zagrożeń[17]. Zapotrzebowanie na ten produkt ubezpieczeniowy jest coraz większe. Niemniej jednak oferty zakładów ubezpieczeń mocno się różnią w zależności od kraju. Generalnie, brak wystarczających danych aktuarialnych jest wskazywany przez różne źródła jako przyczyna ograniczonego sukcesu rynku cyberubezpieczeń. Obecnie różni ubezpieczyciele w różny sposób oceniają ryzyko i biorą pod uwagę wiele czynników ryzyka, obejmujących zarówno aspekty techniczne, jak i organizacyjne firmy.

Uwzględnienie cyberbezpieczeństwa w portfelu produktów wiąże się z większym ryzykiem dla zakładów ubezpieczeń niż w przypadku innych tradycyjnych rodzajów ubezpieczeń, co znajduje odzwierciedlenie w cenie produktu. Według badania przeprowadzonego w Wielkiej Brytanii, koszt ubezpieczenia cybernetycznego w stosunku do wykupionego limitu jest zazwyczaj trzykrotnie wyższy niż koszt ubezpieczenia od bardziej znanych ryzyk odpowiedzialności cywilnej ogólnej i sześciokrotnie wyższy niż w przypadku ubezpieczenia mienia[18].

Produkty ubezpieczeniowe, oferowane przez zakłady ubezpieczeń w Polsce, obejmują różnorodne szkody pochodzenia cybernetycznego, w szczególności z tytułu:

- roszczenia, które zostało podniesione po raz pierwszy przeciwko firmie (Ubezpieczonemu) w okresie ubezpieczenia. Podstawą roszczenia może być postępowanie cywilne, karne, administracyjne lub arbitrażowe wszczęte przeciwko przedsiębiorstwu (Ubezpieczonemu) dotyczące uzyskania odszkodowania lub nałożenia sankcji wskutek przypadku naruszenia danych, przypadku naruszenia związanego z działalnością multimedialną lub przypadku zagrożenia dla bezpieczeństwa sieci. Warto szczególnie podkreślić szkody wyrządzone osobom trzecim w następstwie ataku komputerowego, za który ponosi odpowiedzialność przedsiębiorstwo w związku z wykonywaniem czynności związanych z wprowadzaniem lub przetwarzaniem danych elektronicznych dla celów wykonywania własnej działalności gospodarczej;

[16] R. Böhme, G. Schwartz, *Modeling cyber-insurance: towards a unifying framework*. [w]: Workshop on the Economics in Information Security, WEIS, Harvard University, Cambridge, 7-8 June 2010.

[17] C. Biener, M. Eling, J.H. Wirfs, *Insurability of cyber risk: an empirical analysis*. „Geneva Paper of Risk and Insurance”, 2015, iss. 40(1), p. 3.

[18] UK cyber security: *The role of insurance in managing and mitigating the risk*. https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance (dostęp: 10.04.2022 r.)

- zakłócenia działalności (utraty zysku netto lub zwiększonych wydatków niezbędnych do podtrzymywania działalności przedsiębiorstwa) spowodowanej zdarzeniem cybernetycznym powodującym niezaplanowane wyłączenie systemu komputerowego, zakłócenie lub pogorszenie stanu sieci informatycznej ubezpieczonego przedsiębiorstwa lub sieci informatycznej któregokolwiek z dostawców usług w chmurze. Takie wydarzenie mogło zrealizować się z datą wsteczną, ale decydującym jest to, że podmiot ubezpieczony dowiedział się o tym w okresie ubezpieczenia;
- kosztów naprawienia poniesionych przez ubezpieczone przedsiębiorstwo w wyniku zaistniałego lub zagrażającego przypadku naruszenia danych lub przypadku zagrożenia dla bezpieczeństwa sieci. Do kosztów naprawienia najczęściej się zalicza koszty monitorowania transakcji, koszty odtworzenia, odzyskania lub ponownego zainstalowania danych, koszty śledztwa oraz koszty obsługi prawnej;
- kosztów kar i oceny według *Payment Card Industry* na skutek przypadku naruszenia danych. Należą do nich wszelkie kwoty, jakie zgodnie z prawem przedsiębiorstwo (Ubezpieczony) będzie zobowiązane zapłacić na podstawie umowy o usługi handlowe w następstwie naruszenia danych stanowiącego pogwałcenie standardów bezpieczeństwa danych branży kart płatniczych (*Payment Card Industry Data Security Standa*rd)[19], w tym kary, opłaty za prowadzenie sprawy, opłaty za niezgodność z przepisami, zwrot kwot z bezprawnych transakcji;
- kosztów reakcji, obejmujących uzasadnione i niezbędne opłaty oraz wydatki zewnętrznego eksperta, związanych z ustalaniem przyczyn powstania naruszenia prywatności lub danych. Do zakresu obowiązków eksperta należy analiza systemu komputerowego przedsiębiorstwa, podjęcie działań prewencyjnych, zabezpieczenie danych w systemie komputerowym, określenia zakresu wszelkich właściwych zobowiązań odszkodowawczych, założenie i pozyskanie nowych numerów kont, monitoring transakcji, itp.;
- szkód wynikających z cyberwymuszenia – kwoty zapłacone w celu usunięcia lub przerwania zagrożenia cyberwymuszenia;
- koszty zawiadamiania poszkodowanych oraz innych właściwych osób, wynajęcia infolinii w celu m.in. poinformowania klientów o wycieku danych osobowych;

[19] Do takich podmiotów należą American Express, Mastercard, Visa, Maestro Card lub inny usługodawca dopuszczony przez właściwy organ nadzorujący do świadczenia usług płatniczych.

– koszty ochrony dobrego imienia (Public Relations w celu minimalizacji szkód reputacyjnych).

W każdym z wymienionych punktów istotnym jest warunek ustalający moment w którym przedsiębiorstwo (Ubezpieczony) dowiedziało się o fakcie zaistniałej szkody. Dla celów uzyskania prawa do odszkodowania taki moment jako i bezpośrednie zgłoszenie szkody powinien się mieścić w okresie ubezpieczenia.

5. Wnioski

Rozwój cyberubezpieczeń w dużym stopniu zależy od możliwości zdefiniowania zagrożeń i określenia potencjalnych szkód przez zakłady ubezpieczeń. Przegląd ogólnych warunków ubezpieczeń wybranych ubezpieczycieli (PZU S.A, ERGO Hestia S.A., Allianz S.A. i Generalli Polska TU S.A.) wykazał, że nie istnieje jednolita klasyfikacja ryzyka cybernetycznego jako zdarzenia ubezpieczeniowego. Ryzyko cybernetyczne może występować w postaci niezamierzonego wycieku danych, utraty prywatności, złośliwych prób uszkodzenia systemów cyfrowych, złośliwych prób kradzieży lub zmiany poufnych danych firmowych w celu uzyskania korzyści ekonomicznych, a nawet w postaci kampanii dezinformacyjnych. Szkody mogą być sporadyczne lub mieć charakter globalny i dotyczyć globalnych zasobów cyfrowych (DOS lub DDOS). Istnieje całe spektrum ryzyka cybernetycznego, z którym może zetknąć się przedsiębiorstwo – od niezamierzonego wycieku danych po strategiczne ataki państw narodowych. Zakres ryzyka cybernetycznego jest trudny do scharakteryzowania, ponieważ panuje powszechna wielowymiarowość tego, co właściwie oznacza zdarzenie cybernetyczne.

Z punktu widzenia ochrony ubezpieczeniowej, dla celów stworzenia bazy danych na temat ryzyka cybernetycznego kluczowe znaczenie ma posiadanie jasnej i spójnej terminologii dotyczącej zdarzeń cybernetycznych i ich potencjalnych skutków. Problem tkwi w zakresie określenia ryzyka cybernetycznego, gdy podejścia ubezpieczycieli są bardzo różne. Najczęściej w zakresie ryzyka znajdują się naruszenie bezpieczeństwa sieci, naruszenie prywatności, nieprawidłowe zachowanie związane z działalnością medialną, cyberatak i cyberkradzież.

Jak pokazała analiza ofert zakładów ubezpieczeń w Polsce, zakres odpowiedzialności jest podobny i obejmuje roszczenia od osób trzecich oraz koszty różnych działań ukierunkowanych na powrót danych do stanu sprzed cyberincydentu. Ochroną mogą zostać objęte dodatkowe koszty, które powstają bezpośrednio wskutek incydentu (na przykład koszt porady prawnej).

BIBLIOGRAFIA

Literatura

Biener C., Eling M., Wirfs J.H., *Insurability of cyber risk: an empirical analysis*, „Geneva Paper Risk and Insurance", 2015, iss. 40(1).

Böhme R., Schwartz G., *Modeling cyber-insurance: towards a unifying framework*. [w]: *Workshop on the Economics in Information Security*, WEIS, Harvard University, Cambridge, 7-8 June 2010.

Boyer M., *Cyber insurance demand, supply, contracts and cases*, „The Geneva Papers on Risk and Insurance – Issues and Practice", 2020, vol. 45.

Brenner S. W., *History of computer crime*, [w:] *The history of information security*, red. K.de Leeuw, J. Bergstra, Wydawnictwo Elsevier, Amsterdam 2007.

DeNardis L., *A history of internet security*. [w:] *The history of information security*, red. K.de Leeuw, J. Bergstra, Wydawnictwo Elsevier, Amsterdam 2007.

Kshetri N., *The evolution of cyber-insurance industry and marke: An institutional analysis*, „Telecommunications Policy" September 2020, vol. 44, iss. 8.

Pogrebna G., M.Skilton, *Cybersecurity Threats: Past and Present*, [w:] *Navigating New Cyber Risks*, red. G. Pogrebna, M. Skilton, Palgrave Macmillan, Cham 2019.

Refsdal A., Solhaug B., Stølen K., *Cyber-risk Management*, Springer Briefs in Computer Science. Springer, Cham 2015.

Romanosky S., Ablon L., Kuehn A., Jones T., *Content analysis of cyber insurance policies: how do carriers prices cyber risk*?, „Journal od Cybersecurity", 2019, vol. 5, iss. 1.

Strupczewski G., *Defining cyber risk*, „Safety science", 2021, nr 135.

Inne

Cost of Data Breach Report 2021, IBM Security &Ponemon Institute, https://www.ibm.com/security/data-breach (dostęp: 14.02.2022 r.).

Deloitte Center for Financial Services, *Demystifing cyber insurance coverage report*, 2017, https://www2.deloitte.com (dostęp: 14.02.2022 r.).

Hartwig R. P., Wilkinson C., *Cyber risks: The growing threat*, Insurance Information Institute, June 2014, http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf. (dostęp: 14.02.2022 r.).

Johansmeyer T., *The cyber insurance market needs more money*, March 10, 2022, Harvard Business Review, https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money (dostęp: 14.02.2022 r.).

NetDilgence: *Netdiligence cyber claims study 2014*. Technical report, NetDilligence (2014), https://www.netdiligence.com (dostęp: 10.04.2022 r.)

Ogólne warunki ubezpieczeń, https://cyberochrona.ergohestia.pl/cyber-m/ (dostęp: 10.04.2022 r.).

Ogólne warunki ubezpieczeń, https://www.allianz.pl/content/dam/onemarketing/cee/azpl/dokumenty/dla-firm/ryzyka-finansowe/cyber/CYBER_owu.pdf (dostęp: 10.04.2022 r.).

Ogólne warunki ubezpieczeń, https://www.generali.pl/dla-firmy/majatek/duze-przedsiebiorstwa (dostęp: 10.04.2022 r.).

Ogólne warunki ubezpieczeń, https://www.pzu.pl/_fileserver/item/1515773 (dostęp: 10.04.2022 r.).

Report on the Cybersecurity Insurance Market – NAIC, https://content.naic.org › sites › default › files (dostęp: 10.04.2022 r.)

UK cyber security: *The role of insurance in managing and mitigating the risk*. https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance (dostęp: 10.04.2022 r.).