MISCELLANEA

Bank i Kredyt 54(5), 2023, 557-576

BANK I KREDYT
BANK & CREDIT

Cyberbezpieczeństwo polskiego sektora ubezpieczeniowego w kontekście krajowych i unijnych regulacji prawnych

Piotr Pisarewicz*, Jerzy Podlewski#

Nadesłany: 18 marca 2023 r. Zaakceptowany: 31 lipca 2023 r.

Streszczenie

Celem głównym niniejszego opracowania jest analiza obecnej sytuacji w zakresie przepisów prawnych związanych z bezpieczeństwem teleinformatycznym zakładów ubezpieczeń. Celami szczegółowymi są natomiast: analiza ilościowa danych rynkowych dotyczących ryzyka teleinformatycznego oraz odpowiedź na pytanie, czy nowe regulacje przyczynią się do wzrostu bezpieczeństwa sektora ubezpieczeniowego. W artykule omówiono zagadnienia z uwzględnieniem nowej perspektywy regulacyjnej. Dużą rolę w zwiększaniu bezpieczeństwa systemowego odegra w najbliższych latach nowe rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA), które weszło w życie na początku 2023 r. Jego wdrożenie spowoduje dostosowanie krajowych regulacji do nowych standardów bezpieczeństwa do stycznia 2025 r. Obecne wymagania ustawowe, wytyczne KNF oraz nowe regulacje unijne w praktyce są podstawą bezpieczeństwa oraz jakości oferowanych usług finansowych. Poruszane w artykule zagadnienia mają i będą miały znaczenie dla bieżącego funkcjonowania zakładów ubezpieczeń.

Słowa kluczowe: bezpieczeństwo, cyberataki, ICT, zakłady ubezpieczeń, regulacje prawne, wytyczne i rekomendacje, KNF

JEL: D14, D91, G53, G41

* Uniwersytet Gdański; e-mail: piotr.pisarewicz@ug.edu.pl; ORCID: 0000-0003-1983-1499.
# Uniwersytet Gdański; e-mail: jerzy.podlewski@ug.edu.pl; ORCID: 0000-0001-9571-5540.

1. Wprowadzenie

Sektor ubezpieczeniowy odgrywa, obok sektora bankowego, bardzo ważną rolę na rynku finansowym. Usługi świadczone przez zakłady ubezpieczeń są istotne nie tylko dla klientów indywidualnych, lecz także dla odbiorców instytucjonalnych. Z tego względu muszą być oferowane z zachowaniem najwyższych standardów bezpieczeństwa, wynikających zarówno z regulacji prawnych, jak i wymogów narzuconych przez rynek.

Aby osiągnąć te standardy, podmioty stosują wiele procedur, które mają na celu zachowanie ich zgodności z literą, a niejednokrotnie także z duchem prawa, ponieważ niektóre zapisy ustawowe wydają się dosyć ogólne. W tym celu Komisja Nadzoru Finansowego (KNF) tworzy bardziej szczegółowe dokumenty, których zadaniem jest doprecyzowanie zapisów ustawowych oraz osiągnięcie maksymalnego bezpieczeństwa działalności operacyjnej. Pozwalają one uniknąć wielu negatywnych skutków ryzyka operacyjnego, które może się zmaterializować w formie straty wynikającej z niewłaściwych lub błędnych procesów wewnętrznych, działań personelu lub systemów, a także zdarzeń zewnętrznych.

Głównym celem niniejszego opracowania jest analiza obecnej sytuacji w zakresie przepisów prawa związanych z bezpieczeństwem teleinformatycznym zakładów ubezpieczeń. Celami szczegółowymi są natomiast: analiza ilościowa danych rynkowych w zakresie ryzyka teleinformatycznego oraz odpowiedź na pytanie, czy nowe regulacje przyczynią się do wzrostu bezpieczeństwa sektora ubezpieczeniowego. Wnioski wynikające z realizacji celu głównego i celów szczegółowych mogą być w praktyce inspiracją dla władz zakładów ubezpieczeń, poszukujących najbardziej adekwatnych metod zarządzania ryzykiem cybernetycznym, zapobiegania mu oraz ograniczania jego skutków. Bezpieczeństwo teleinformatyczne i bezpieczeństwo cybernetyczne są w literaturze przedmiotu oraz w niniejszym artykule pojęciami stosowanymi zamiennie lub wspólnie w zależności od kontekstu bądź rodzajów zagrożeń.

W analizowanym obszarze w najbliższych latach szczególną rolę odegra nowe rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act), które weszło w życie na początku 2023 r. Do stycznia 2025 r. należy dostosować krajowe regulacje do nowych wymogów, które mają za zadanie podwyższenie poziomu bezpieczeństwa sektora ubezpieczeniowego oraz całego rynku finansowego. Celem regulacji omawianych w niniejszym artykule oraz działań podejmowanych przez instytucje finansowe jest zwiększenie bezpieczeństwa oferowanych usług. W artykule omówiono obowiązujące regulacje prawne, ze szczególnym uwzględnieniem najnowszych regulacji Unii Europejskiej i regulacji KNF stanowiących doprecyzowanie istniejących przepisów ustawowych w formie tzw. miękkiego prawa.

Problematyka poruszana w artykule ma zastosowanie praktyczne, ponieważ wszystkie regulacje muszą być przestrzegane w bieżącym funkcjonowaniu zakładów ubezpieczeń. W przeciwnym wypadku KNF może interweniować i żądać od ubezpieczyciela wyjaśnień, a także zapewnienia, że niestosowanie niektórych elementów wytycznych lub rekomendacji jest uzasadnione i nie powoduje negatywnych konsekwencji dla niego i/lub jego klientów. Wykorzystane w artykule metody badawcze to: analiza krytyczna literatury, dedukcja jako sposób wnioskowania teoretycznego oraz indukcja zastosowana do analizy opisowej i statystycznej.

2. Bezpieczeństwo teleinformatyczne i zagrożenia cybernetyczne w sektorze ubezpieczeniowym

Szeroko rozumiane zarządzanie bezpieczeństwem oferowanych produktów i usług to jeden z najważniejszych paradygmatów i wyznaczników dojrzałego zarządzania przedsiębiorstwem. Zagadnienie to ma charakter wielowątkowy i interdyscyplinarny. Pojęcie bezpieczeństwa nie jest niczym nowym i funkcjonuje w języku codziennym. Oznacza brak zagrożenia, poczucie pewności i komfortu życia, wolności od zagrożeń oraz wiarę w skuteczność pomocy. Jednak dopiero na przełomie ubiegłego wieku wzrosło zainteresowanie tą tematyką. Bezpieczeństwo stało się wtedy przedmiotem badań naukowych i zastosowań w postaci „zarządzania bezpieczeństwem" (Kuhlmann 1986; Li, Guldenmund 2018, s. 94–123).

Koziej (2011, s. 19–41) oraz Cieślarczyk (2011, s. 17–18) zwrócili uwagę, że termin „bezpieczeństwo" ma zarówno charakter statyczny (stan), jak i dynamiczny – proces zapewniania bezpieczeństwa. Typologie bezpieczeństwa wymieniają jego rodzaje m.in. z punktu widzenia podmiotowego (bezpieczeństwo narodowe i międzynarodowe), przedmiotowego (polityczne, gospodarcze, informacyjne, cybernetyczne itp.), przestrzennego (lokalne, globalne itp.) czy perspektywy organizacyjnej (Hale, Baram 1998, s. 3–11; Kaczmarczyk 2013, s. 20–21). Można wskazać wiele analiz zagrożeń dla bezpieczeństwa i ich rankingów. Mają one postać mniej lub bardziej rozbudowanych opracowań, przygotowywanych cyklicznie przez ośrodki badawcze, globalne think tanki, takie jak Economist Intelligence Unit (EIU 2022), jak też firmy doradcze (Eurasia Group 2022). Jedną z najbardziej znanych analiz zagrożeń globalnych jest doroczny Global Risk Report Światowego Forum Ekonomicznego (WEF 2022). Analiza zagrożeń dla bezpieczeństwa jest szczególnie ważna dla towarzystw ubezpieczeniowych, w których ryzyko jest niejako podstawową materią działalności. Przykładem jest Allianz Risk Barometer, którego wydanie z 2022 r. jest efektem badania przeprowadzonego wśród 2650 ekspertów w 89 krajach. Według respondentów Allianz najważniejsze rodzaje ryzyka, które będą wpływały na gospodarkę światową w 2022 r., wiążą się z technologią komputerową. Są to kolejno: oprogramowanie wyłudzające okup, wykradzenie danych, ryzyko wynikające z telepracy, cyfrowe zagrożenia dla łańcuchów dostaw oraz chmur obliczeniowych (Allianz 2022).

Bezpieczeństwo teleinformatyczne i cybernetyczne to pojęcia stosowane w literaturze przedmiotu wspólnie bądź zamiennie. Rozumie się przez nie różne rodzaje zagrożeń, które niesie rozwój technologii komunikacyjnych oraz ich wykorzystywanie przez użytkowników ze wszystkich sektorów gospodarki narodowej i przez gospodarstwa domowe (Eger 1981, s. 204–205; Craigen, Diakun-Thibault, Purse 2014; Gupta, Goyal 2020, s. 18). Według klasyfikacji przedmiotowej bezpieczeństwo teleinformatyczne to pojęcie szerokie i obejmuje utratę (zagrożenie) poufności, integralności i dostępności danych oraz systemów informatycznych. Zagrożenia te mogą być wywoływane zarówno świadomym, jak i nieświadomym działaniem człowieka oraz różnego rodzaju problemami technicznymi (Pałęga i in. 2013, s. 265). Wymieniane są również zagrożenia związane z autentycznością, odpowiedzialnością, niezaprzeczalnością oraz niezawodnością danych i systemów (EIOPA 2020).

Bezpieczeństwo teleinformatyczne obejmuje również zdarzenia o typowo operacyjnym charakterze, wywoływane czynnikami zewnętrznymi (np. pożar, zalanie serwerów komputerowych czy przerwa w dostawie energii). Tego rodzaju zagrożenia są w istocie dobrze znane i – nie umniejszając ich znaczenia – stosunkowo łatwo nimi zarządzać.

Należy zauważyć, że pojęcie cyberprzestrzeni jest niełatwe do zdefiniowania, bowiem jego zakres i stopień złożoności nieustannie się zmieniają w związku z rozwojem Internetu i obszarów z nim związanych, takich jak Internet rzeczy, *big data*, *cloud computing*, robotyka czy sztuczna inteligencja (AI). W Polsce rządowa *Doktryna bezpieczeństwa Rzeczypospolitej Polskiej* definiuje cyberprzestrzeń jako „przestrzeń przetwarzania i wymiany informacji tworzonych przez systemy teleinformatyczne", a cyberbezpieczeństwo jako „proces zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni" (BBN 2015, s. 7). Dokument jest wyrazem regulacyjnego i strategicznego podejścia do bezpieczeństwa teleinformatycznego, które wraz z samoregulacją i dobrymi praktykami odgrywa niezwykle ważną rolę w zapewnieniu bezpieczeństwa w ogóle, nie tylko w obszarze cybernetycznym (Chochowski 2019).

Zagadnienie cyberbezpieczeństwa jest niezmiernie istotne również dlatego, że celem cyberataków jest infrastruktura krytyczna, elementy systemów finansowych państw i cała gospodarka. Cyberataki są coraz częściej dokonywane bądź inicjowane przez służby Rosji, Białorusi i Korei Północnej (Hoffmann 2018, s. 71–78; Youchong, Quingui 2021, s. 8180). W związku z wojną w Ukrainie cyberbezpieczeństwo, szczególnie w sektorze finansowym, staje się fundamentalnym elementem systemu obrony narodowej.

Z szeroko pojętym, strategicznym cyberbezpieczeństwem wiąże się wspomniane rozporządzenie DORA, którego przygotowanie rozpoczęło się kilka lat temu (Kuna 2020). Jego rola została już opisana w polskiej literaturze przedmiotu. Autorzy z jednej strony doceniają jego znaczenie i możliwy długofalowy wkład we wzrost poziomu bezpieczeństwa. Z drugiej strony wskazują, że niektóre jego przepisy są zbieżne z istniejącymi regulacjami, w szczególności wytycznymi i rekomendacjami KNF (Węgrzyn 2021; Pelc 2021; Ruiz 2022; Kulesza, Racki 2022; Kulesza, Filipowski 2022).

Znaczenie rozporządzenia wynika prawdopodobnie z jego kompleksowości, co przyczyni się do usystematyzowania istniejących regulacji i uzupełnienia ich o nowe treści. Ze względu na przyjętą w nim zasadę proporcjonalności stosowanie rozporządzenia nie powinno się jednak wiązać z bardzo uciążliwymi procedurami dostosowawczymi, nawet w mniejszych podmiotach.

3. Incydenty naruszenia cyberbezpieczeństwa oraz ich koszty

Łączne globalne koszty różnego rodzaju cyberataków w 2022 r. szacowano na 8,4 bln USD, tymczasem jeszcze w 2018 r. były 10-krotnie mniejsze (tabela 1). Największy przyrost zanotowano w 2020 r. – pierwszym roku pandemii COVID-19. Wzrosły wówczas o 154% w stosunku do poprzedniego roku, do 2,9 bln USD. Do 2027 r. przewidywane koszty mogą przekroczyć 23,8 bln USD (Statista 2022), a ich łączna wielkość w latach 2016–2027 może osiągnąć 109 bln USD. Wartości te pokazują skalę problemu, przed którym stoi światowa gospodarka i wszystkie branże działające na rynkach międzynarodowych. Prognozowanie w tym obszarze jest jednak bardzo trudne ze względu na szybki postęp technologiczny, przede wszystkim zmiany w obszarze sztucznej inteligencji, która jest używana zarówno do przeprowadzania ataków, jak i obrony przed nimi (Zouave i in. 2020; Mosteanu 2020, s. 148–156).

Sektor finansowy należy do głównych celów cyberataków na świecie, ale sektor ubezpieczeniowy jest rzadziej atakowany niż banki. Wynika to ze specyfiki działalności zakładów ubezpieczeń, które wydają się mniej atrakcyjne dla przestępców niż banki czy inne instytucje finansowe. Typowe zagrożenia dla bezpieczeństwa funkcjonowania systemów teleinformatycznych ubezpieczycieli są następujące:

– utrata i/lub kradzież poufnych danych,

– *phishing* – rodzaj ataku kombinowanego, na który składają się: przygotowanie fałszywej strony internetowej oraz działania socjotechniczne mające na celu wyłudzanie informacji od atakowanego podmiotu lub skorzystanie przez niego z oferowanych usług,

– *ransomware* – szkodliwe oprogramowanie powodujące utratę dostępu do informacji, za którego przywrócenie atakujący żąda okupu,

– *cryptojacking* („złośliwe wydobywanie kryptowalut") – program ukrywający się w komputerze lub urządzeniu przenośnym i wykorzystujący jego zasoby do „wydobywania" kryptowalut,

– DDoS (*distributed denial of service* – rozproszony atak odmowy usług); jego wynikiem jest uniemożliwienie uprawnionym podmiotom dostępu do zasobów lub jego znaczne spowolnienie, często przy wykorzystaniu wielu źródeł ataku – np. komputerów połączonych w sieć, zwykle w postaci botnetu,

– *SQL injection* – „wstrzyknięcie" danych, zmuszających aplikację do nieprawidłowego, często szkodliwego działania,

– *zero day exploit* – atak wykorzystujący lukę w zabezpieczeniach oprogramowania producenta, zanim zostanie ujawniona[1],

– nieautoryzowane transakcje i kradzieże funduszy,

– cyberataki i problemy z systemami informacyjnymi w łańcuchach dostaw oraz w dystrybucji usług ubezpieczeniowych (EIOPA 2019; Vecto 2020).

Ogólna liczba różnego rodzaju cyberataków Polsce w latach 1996–2021 wzrosła z 50 w 1996 r. do 29 483 w 2021 r. Najszybszy wzrost zanotowano w okresie pandemii w 2021 r. – o 183% w stosunku do 2020 r. (tabela 2). Bliższa analiza dostępnych danych wskazuje, że w Polsce w 2019 r. w sektorze ubezpieczeniowym stwierdzono pięć, w 2020 r. dwa, a w 2021 r. jedynie trzy cyberincydenty (tabela 3). Dla porównania w sektorze bankowym takich zdarzeń było odpowiednio: 1057, 1008 i 947. Taka statystyka – przy założeniu, że obejmuje wszystkie dane rynkowe – stawia ubezpieczenia na równi z mniej zagrożonymi branżami i daje im 25. pozycję w rankingu zagrożonych branż (na 28 sklasyfikowanych). Sektor bankowy znalazł się na siódmym miejscu w Polsce, gdzie trzy najbardziej zagrożone sektory to: media, handel oraz usługi pocztowe i kurierskie (CERT Polska 2022). Również badanie przeprowadzone przez Związek Banków Polskich potwierdziło (choć nie wprost), że sektor ubezpieczeniowy jest mniej narażony na cyberataki niż bankowość. Wskazano w nim banki jako „liderów" w obszarze cyberbezpieczeństwa, natomiast firmy ubezpieczeniowe znalazły się na szóstej pozycji (ZBP 2020). Zakładając, że ubezpieczyciele mają profesjonalne podejście do spraw cyberbezpieczeństwa, może to sugerować słabsze zagrożenie cyberatakami, a tym samym konieczność stosowania mniej wyrafinowanych zabezpieczeń niż w przypadku banków.

Oczywiście oficjalnie liczba cyberincydentów w sektorze ubezpieczeniowym nie musi dokładnie odzwierciedlać rzeczywistej liczby cyberataków, lecz jedynie te zaraportowane, a przede wszystkim wykryte. Problem ten dotyczy ujawniania cyberataków w ogóle. Opinia publiczna i badacze problemu dowiadywali się o nich niejednokrotnie dopiero wtedy, kiedy nie dało się ich ukryć. Tak było w przypadku jednego z głośniejszych cyberataków w historii, którego ofiarą padł amerykański ubezpieczyciel Anthem w 2015 r. (Walters 2015). Z kolei w 2017 r. nastąpił atak cybernetyczny na stronę internetową KNF, który miał doprowadzić do kradzieży bliżej nieokreślonej ilości danych dotyczących instytucji

[1] Narodowy Standard Cyberbezpieczeństwa, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa,* Pełnomocnik Rządu ds. Cyberbezpieczeństwa*;* https://www.intel.pl/content/www/pl/pl/business/enterprise-computers/resources/what-is-a-zero-day-exploit.html.

finansowych w Polsce. Wykorzystano do tego prawdopodobnie metodę wodopoju (tzw. *watering hole*), czyli źródła infekującego komputery użytkowników. Do tej pory okoliczności i skutki tego ataku pozostają niejasne. Ani KNF, ani ewentualnie zaatakowane instytucje nie ujawniły zakresu ataku i wysokości szkód. Pojawiły się natomiast niesprawdzone informacje, że złośliwy kod znaleziono w 20 polskich bankach, a sponsorem ataku mogła być Korea Północna (Mozur, Sang-Hun 2017; Niebezpiecznik 2017).

Jeśli chodzi o rodzaje cyberataków, to według analiz CERT (CERT Polska 2022) w 2021 r. w Polsce najczęstsze były: fraudy (oszustwa, wyłudzenia) – 25 472 przypadki (wzrost o 523 % w stosunku do 2019 r.), złośliwe oprogramowanie – 2847 (wzrost o 193%), obraźliwe i nielegalne treści – 311 (spadek o 161%), włamania do systemów – 247 (wzrost o 54%) (tabela 4).

Z kolei KPMG (KPMG 2022, s. 11) zleciło przeprowadzenie badania ankietowego wśród 100 polskich przedsiębiorstw, w którym uszeregowano zagrożenia cybernetyczne według skali ryzyka od 1 do 5 (1 to najmniejsze, a 5 to największe ryzyko). Najwięcej respondentów (13%) wskazało, że z najpoważniejszym ryzykiem wiążą się: kradzież danych oraz tzw. zaawansowane trwałe zagrożenie (APT, *advanced persistent threat*), natomiast 11% wskazało na *phishing*, a 8% na wyciek danych i złośliwe oprogramowanie. Za najmniej ryzykowne respondenci uznali ataki typu DDoS – tylko 1% przypisał im ryzyko o najwyższej wartości (tabela 5).

4. Bezpieczeństwo teleinformatyczne a obecny stan regulacji sektora ubezpieczeniowego

Jakość oferowanych produktów finansowych w znacznym stopniu zależy od zaawansowania oraz bezpieczeństwa systemów informatycznych. Czynnik ten odgrywa coraz większą rolę w funkcjonowaniu wszystkich instytucji finansowych. Zakłady ubezpieczeń, podobnie jak pozostałe instytucje finansowe, muszą spełnić szereg wymogów oraz opracować wiele procedur, mających na celu prowadzenie działalności zgodnie z najwyższymi standardami bezpieczeństwa finansowego, operacyjnego oraz jakości świadczonych usług. Należy wspomnieć, że akty prawne regulujące sektor ubezpieczeniowy w Polsce liczą kilkadziesiąt różnych ustaw i rozporządzeń. Świadczy to o złożoności systemu oraz wymagań, które muszą zostać spełnione przez rodzime podmioty. Szeroki zakres wymogów niejednokrotnie sprawia problemy z ich stosowaniem, ponieważ niektóre zapisy ustawowe wydają się zbyt ogólnikowe.

KNF opracowuje bardziej szczegółowe dokumenty (rekomendacje, wytyczne), których intencją jest doprecyzowanie zapisów ustawowych oraz jak najwyższa jakość i bezpieczeństwo działalności operacyjnej. Bardziej szczegółowymi celami regulacji nadzorczych są: zapewnienie zgodności działania z przepisami prawa, zapobieżenie naruszaniu interesów ubezpieczających, ubezpieczonych lub uprawnionych z umów ubezpieczenia oraz ograniczenie ryzyka działalności zakładów ubezpieczeń.

KNF tworzy je na podstawie zapisów Ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej. W praktyce regulacje KNF powinny być stosowane w zależności od specyfiki, skali i charakteru działania każdego podmiotu. Zasada, którą kieruje się polski nadzorca, to: „zastosuj lub wyjaśnij". Oznacza to, że podmioty, które nie dostosują się do wymogów KNF, powinny poinformować o tym fakcie, wyjaśniając przyczyny takiego stanu rzeczy. Muszą także poinformować, jak zamierzają osiągnąć cele wskazane w rekomendacjach lub wytycznych.

Ze względu na praktykę rynkową niewiele podmiotów decyduje się na nierespektowanie tych regulacji, ponieważ może to grozić długotrwałymi sporami z organem nadzoru i pośrednio spowodować również zwiększoną aktywność kontrolną.

W obszarze szeroko rozumianego bezpieczeństwa teleinformatycznego obowiązują obecnie wytyczne KNF z 2014 r. dotyczące zarządzania technologią informacyjną i bezpieczeństwem środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji. W myśl tej regulacji KNF systemy informatyczne to tzw. środowisko informatyczne (teleinformatyczne), obejmujące infrastrukturę systemów wspierających działalność instytucji finansowej, opartą na infrastrukturze zapewnianej przez podmioty zewnętrzne. Zgodnie z wytycznymi do infrastruktury teleinformatycznej zalicza się: „zespół urządzeń i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych towarzystwa". System informatyczny jest natomiast aplikacją lub zbiorem powiązanych aplikacji komputerowych, których celem jest przetwarzanie danych.

Bardziej syntetycznie definiuje te pojęcia EIOPA (European Insurance and Occupational Pension Authority) – jako „zestaw aplikacji, usług, zasobów informatycznych, zasobów ICT (technologie informacyjno-komunikacyjne) lub innych elementów przetwarzających informacje, obejmujący np. środowisko operacyjne" (EIOPA 2020).

W funkcjonowaniu systemów informatycznych istnieje wiele obszarów krytycznych dla użytkujących je instytucji. Jednym z nich jest poufność danych zabezpieczająca przed dostępem nieuprawnionych podmiotów lub osób. Według wytycznych KNF najwyższe standardy muszą być zachowane również podczas przetwarzania danych na wszystkich etapach, do których zalicza się: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, a także usuwanie danych.

Wytyczne KNF należy traktować jako zbiór dobrych praktyk, które powinny być stosowane z zachowaniem zasady proporcjonalności. W tym przypadku oznacza ona, że powinny uwzględniać specyfikę ryzyka, charakter środowiska teleinformatycznego oraz relację kosztów ich wprowadzenia do wynikających z tego korzyści. Jednym z kluczowych celów wytycznych jest zapewnienie bezpieczeństwa informacji, czyli poufności danych, ich integralności oraz dostępności. Jak wspomniano, w ostatnich latach coraz częstsze i groźniejsze wydają się ataki cybernetyczne, które niejednokrotnie polegają na żądaniu okupu (*ransomware*). W myśl wytycznych KNF są to tzw. incydenty naruszenia bezpieczeństwa środowiska teleinformatycznego, tj. pojedyncze niepożądane lub niespodziewane zdarzenia bądź serie takich zdarzeń, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji.

Struktura dokumentu KNF obejmuje 22 wytyczne szczegółowe, dotyczące kilku obszarów strategicznych:

– strategii i organizacji obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego – pięć wytycznych,

– rozwoju środowiska teleinformatycznego – dwie wytyczne,

– utrzymania i eksploatacji środowiska teleinformatycznego – 10 wytycznych,

– zarządzania bezpieczeństwem środowiska teleinformatycznego – pięć wytycznych.

Liczba oraz zakres aktów prawnych, a także szczegółowość wytycznych i rekomendacji KNF świadczą o złożoności formalnoprawnych warunków działania sektora ubezpieczeniowego oraz całego rynku finansowego w Polsce.

Rosnąca liczba cyberataków i wszelkiego rodzaju incydentów naruszenia bezpieczeństwa zmusiła organy Unii Europejskiej do podjęcia kolejnych kroków, kompleksowo ujmujących zagadnienia cyberbezpieczeństwa. Działania w tym obszarze zostały wskazane w kolejnej części niniejszego opracowania.

5. Nowe wyzwania w zakresie cyberbezpieczeństwa a harmonizacja regulacji prawnych na poziomie Unii Europejskiej

W ostatnich latach można zaobserwować coraz silniejsze powiązania między podmiotami finansowymi, rynkami finansowymi, infrastrukturami rynku finansowego oraz klientami. Zwiększa to ich podatność na zagrożenie o charakterze systemowym. Lokalne cyberincydenty mogą bardzo szybko objąć każdy z około 22 000 podmiotów finansowych działających w UE, a następnie rozprzestrzenić się na cały system finansowy. Należy zwrócić uwagę, że takie zagrożenia dotyczą nie tylko rynku finansowego, lecz większości sektorów współczesnej gospodarki. Jak wskazano w rozporządzeniu DORA, negatywną konsekwencją dla stabilności unijnego systemu finansowego może być utrata płynności rynków finansowych i zaufania do nich.

Wprawdzie unijny sektor finansowy jest regulowany przez jednolity zbiór przepisów i podlega Europejskiemu Urzędowi Nadzoru Finansowego (European Banking Authority – EBA), jednak przepisy dotyczące operacyjnej odporności cyfrowej i bezpieczeństwa ICT nie zostały w pełni zharmonizowane. Konieczne było zatem włączenie wymogów w zakresie ryzyka ICT do przepisów dotyczących ryzyka operacyjnego zawartych dotychczas w różnych unijnych aktach prawnych.

Aby wyjść naprzeciw nowym wyzwaniom i zapobiegać zagrożeniom dotyczącym świata cyfrowego, organy Unii Europejskiej wprowadziły nowy akt prawny. Jest nim rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego DORA (Digital Operational Resilience Act), opublikowane 27 grudnia 2022 r. w Dzienniku Urzędowym UE. Stanowi ono część pakietu legislacyjnego UE regulującego finanse cyfrowe.

Docelowo na terenie Unii Europejskiej powinna być osiągnięta harmonizacja różnych elementów odporności cybernetycznej przez wprowadzenie bardziej rygorystycznych wymogów w porównaniu z innymi przepisami dotyczącymi usług finansowych. Dotyczy to również zwiększonej harmonizacji w porównaniu z wymogami określonymi w dyrektywie (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej wcześniejsze rozporządzenie z 2014 r. i dyrektywy z 2018 oraz 2016 r. Rozporządzenie DORA stanowi zatem uszczegółowienie i doprecyzowanie tego aktu prawnego.

Celem rozporządzenia jest osiągnięcie wysokiego jednakowego poziomu operacyjnej odporności cyfrowej przez wprowadzenie jednolitych wymogów dotyczących bezpieczeństwa sieci i systemów informatycznych wspierających procesy biznesowe podmiotów finansowych. Implementacja założeń zakłada udoskonalenie i rozwój otoczenia regulacyjnego w obszarze technologii finansowych, a ponadto harmonizację procedur i standardów dotyczących odporności cyfrowej w sektorze finansowym.

Efektem działań wskazanych w rozporządzeniu ma być zatem wzrost odporności podmiotów w sektorze finansowym na zagrożenia związane z technologiami informacyjno-komunikacyjnymi, w tym również na coraz częściej występujące cyberataki.

Rozporządzenie weszło w życie 16 stycznia 2023 r., ale na dostosowanie się do jego wymogów rynek będzie miał czas do 17 stycznia 2025 r. Dokument ujednolica wymagania we wszystkich państwach

członkowskich UE i obejmuje wszystkie kluczowe podmioty działające na rynku finansowym, m.in.: banki, zakłady ubezpieczeń, firmy inwestycyjne, instytucje płatnicze, dostawców technologii i usług ICT.

Powodem wprowadzenia rozporządzenia była konieczność ochrony podmiotów finansowych przed poważnymi zakłóceniami operacyjnymi. Wprowadza ono jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych firm sektora finansowego oraz dostawców usług ICT. Nakłada też wymóg wdrożenia wielu rozwiązań przeciwdziałających zagrożeniom w obszarze ICT, a także utrzymywania ciągłości operacyjnej po atakach i zakłóceniach w tym zakresie.

Przepisy wskazują na możliwość zachowania zasady proporcjonalności w takich obszarach, jak: zarządzanie ryzykiem ICT, zgłaszanie incydentów ICT, testowanie cyfrowej odporności operacyjnej oraz zarządzanie ryzykiem podmiotów trzecich związanych z ICT. Zakłady ubezpieczeń nie będą jednak mogły stosować specjalnego uproszczonego systemu zarządzania ryzykiem ICT.

Stosowanie zasady proporcjonalności przez ubezpieczycieli oraz pośredników będzie musiało uwzględniać: rozmiar, charakter, skalę oraz złożoność usług, działań i operacji, a także ogólny profil ich ryzyka. Należy przypomnieć, że wytyczne EIOPA dotyczące bezpieczeństwa i zarządzania w zakresie technologii informacyjno-komunikacyjnych również zakładają stosowanie zasady proporcjonalności, co wskazuje na pewną ciągłość przepisów w tym zakresie.

Rozporządzenie DORA nakłada na podmioty rynku finansowego obowiązek rejestrowania i klasyfikowania incydentów związanych z usługami ICT, wpływających na stabilność, ciągłość lub jakość usług finansowych. Będą one zgłaszane specjalnie wyznaczonemu podmiotowi działającemu w strukturach UE, odpowiedzialnemu za ich zbieranie i obsługę. Instytucja, która stwierdzi wystąpienie takiego incydentu, będzie miała 24 lub 72 godziny na jego zgłoszenie – zależnie od skali i rodzaju zagrożeń z nim związanych.

Jednym z wymogów rozporządzenia DORA jest testowanie cyfrowej odporności na podstawie analizy ryzyka. Organy nadzoru w poszczególnych krajach będą mogły wskazywać podmioty zobligowane do przeprowadzenia dodatkowych testów penetracyjnych (*threat-led penetration testing* – TLPT). Mają one sprawdzać odporność podmiotu przez kontrolowane próby naruszenia integralności systemów IT.

Wychodząc naprzeciw wymogom zawartym w rozporządzeniu DORA i niejako wyprzedzając jego uchwalenie, Urząd Komisji Nadzoru Finansowego 19 października 2022 r. wydał nowe stanowisko dotyczące działań zakładów ubezpieczeń i reasekuracji w zakresie cyberbezpieczeństwa.

Głównym powodem opracowania tego dokumentu był istotny wzrost zagrożeń dla klientów instytucji finansowych, którzy korzystają z elektronicznych form komunikacji, a także zagrożeń w działalności operacyjnej zakładów ubezpieczeń. Jak wspomniano, do publikacji stanowiska przyczyniła się również perspektywa przyjęcia rozporządzenia DORA. Dostosowanie się do jego przepisów będzie oceniane podczas czynności nadzorczych prowadzonych przez KNF.

Stanowisko UKNF ma dosyć ogólny, kierunkowy charakter i obejmuje sześć obszarów, na które zakłady ubezpieczeń mają zwrócić szczególną uwagę. Kluczowym wskazaniem na początku tego dokumentu jest zasada *security first*, polegająca na: „stawianiu bezpieczeństwa na pierwszym planie i podejmowaniu decyzji dotyczących kształtu procesów i produktów w oparciu o przeprowadzenie rzetelnych analiz ryzyka, które muszą uwzględniać nie tylko kwestie bezpieczeństwa środowiska teleinformatycznego Zakładu, ale również zagrożenia związane z korzystaniem z jego usług przez klientów". Uczestnicy rynku winni zatem wdrożyć i stosować procedury spełniające wszystkie wskazane warunki, aby przeciwdziałać nowym zagrożeniom ze strony cyberprzestępców lub wynikającym z błędnego działania systemów.

Drugim wskazaniem UKNF jest wdrożenie wieloskładnikowego uwierzytelnienia tożsamości klienta w elektronicznych kanałach dostępu do usług. Powinno być stosowane m.in. wówczas, gdy klient zdalnie uzyskuje wgląd w tajemnicę ubezpieczeniową czy dokonuje operacji związanych produktem (np. transfer środków pieniężnych, otwieranie nowych rachunków bankowych). Brak takich procedur został uznany za nieakceptowalne ryzyko.

Trzecie zalecenie UKNF to unikanie aktywnych linków w komunikacji z klientami, które w ostatnich latach są główną metodą dokonywania oszustw przez cyberprzestępców. Podszywają się oni pod instytucje zaufania publicznego w celu wyłudzania danych do logowania, przesyłając aktywne linki i SMS-y przekierowujące do fałszywych stron internetowych, lub zamieszczają informacje w mediach społecznościowych. KNF oczekuje odejścia od takich sposobów komunikacji i zwrócenia uwagi klientów na zagrożenia z tym związane.

Czwarte zagadnienie poruszone w dokumencie UKNF to zabezpieczenia w elektronicznej (mailowej) korespondencji z klientami. Dotychczas stosowane zabezpieczenia i szyfrowanie załączników, np. krótkie hasła, PESEL, data urodzenia, numer telefonu, uznano za nieakceptowalne ryzyko. Oczekiwania UKNF w tym zakresie obejmują szyfrowanie zawierające złożone hasła udostępniane osobnym kanałem komunikacji, np. w SMS, lub indywidualne hasła wprowadzane przez klientów.

Kontrola nad działalnością zewnętrznych usługodawców to kolejny obszar, na którym skupił się UKNF. Zwrócił uwagę, że od wielu lat obowiązują wytyczne KNF dotyczące technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w sektorze ubezpieczeniowym. Wskazał na konieczność stosowania odpowiednich mechanizmów kontroli przeprowadzanych bezpośrednio przez ubezpieczycieli lub przez usługodawców czy audytorów zewnętrznych z zastosowaniem międzynarodowych standardów (np. Statement on Standards for Attestation Engagements nr 16).

Końcowym elementem stanowiska UKNF jest edukacja klientów i budowanie ich świadomości finansowej i ubezpieczeniowej co do standardów cyberbezpieczeństwa. Obecnie przeważa pasywne podejście instytucji finansowych do publikacji na ten temat (np. publikowanie informacji na stronach internetowych). UKNF wskazuje na potrzebę współpracy w tym zakresie ze szkołami, środowiskiem akademickim czy instytucjami konsumenckimi, co ma się przyczynić do wzrostu bezpieczeństwa klientów.

6. Podsumowanie

Współczesny rynek finansowy stawia wiele wyzwań działającym na nim podmiotom. Niezależnie od tego, czy jest to bank, fundusz inwestycyjny czy zakład ubezpieczeń, muszą one spełnić wiele wymogów formalnoprawnych oraz finansowych, które zapewnią klientom odpowiedni poziom jakości usług i bezpieczeństwa powierzanych środków. Sektor ubezpieczeń pełni tutaj szczególną rolę, ponieważ oferuje usługi, które wiążą się z zapewnieniem bezpieczeństwa osób fizycznych i organizacji. Ubezpieczyciele wykorzystują wiele metod, technik i dobrych praktyk zarządzania jakością oraz wdrażają normy zarządzania jakością. Jednym z przykładów jest omawiane tu bezpieczeństwo teleinformatyczne.

Jakość świadczonych usług wiąże się z koniecznością zachowania najwyższego poziomu bezpieczeństwa operacyjnego i finansowego zakładów ubezpieczeń. To z kolei wymaga rozbudowanych regulacji prawnych, obejmujących każdy aspekt ich działalności. Ze względu na specyfikę i duży stopień skomplikowania usług podmioty te są objęte różnego typu aktami prawnymi.

Regulacje dotyczące sektora ubezpieczeniowego uwzględniają bezpieczeństwo teleinformatyczne i związane z nim cyberbezpieczeństwo. Kwestie regulacyjne są znacznym wyzwaniem ze względu na niesłychanie szybki rozwój technologii cyfrowych i, co za tym idzie, zagrożeń dla bezpieczeństwa danych przetwarzanych przez ubezpieczycieli, środków, którymi operują, oraz ich funkcjonowania.

Należy pamiętać, że Komisja Nadzoru Finansowego już wcześniej wskazywała na konieczność zgłaszania incydentów naruszania bezpieczeństwa czy przeprowadzania testów penetracyjnych. Można więc założyć, że sektor ubezpieczeniowy w Polsce jest częściowo przygotowany na niedawno wprowadzone przepisy. Skala dostosowań i związanych z nimi kosztów jest jednak trudna do oszacowania, ponieważ każdy podmiot ma inne uwarunkowania i strukturę działalności operacyjnej. Nowe wymogi nie przyczynią się zatem do rewolucyjnych zmian w działalności operacyjnej, ale niewątpliwie podniosą poprzeczkę i zwiększą poziom bezpieczeństwa sektora ubezpieczeniowego oraz całego rynku finansowego.

Odnosząc się do celu głównego oraz celów szczegółowych niniejszego opracowania, autorzy wskazują następujące wnioski i rekomendacje wynikające z przeprowadzonych badań:

- Analiza ilościowa danych rynkowych na temat skali incydentów i ataków cybernetycznych wskazuje na ich systematyczny wzrost w sektorze finansowym, w tym w sektorze ubezpieczeniowym.
- Dotychczasowe regulacje, w szczególności rekomendacje KNF, stanowią podstawę tworzenia procedur w zakresie bezpieczeństwa teleinformatycznego zakładów ubezpieczeń, co przyczyni się do efektywniejszego wdrażania wymogów wskazanych w nowych regulacjach.
- Szczególną rolę w koordynacji działań na rzecz wzrostu bezpieczeństwa systemowego odegra w najbliższych latach nowe rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act), które weszło w życie na początku 2023 r. Konieczne będzie dostosowanie do niego krajowych regulacji prawnych do stycznia 2025 r.
- Obecne wymagania ustawowe, wytyczne KNF i nowe regulacje unijne stanowią podstawę dalszego wzrostu bezpieczeństwa oraz jakości oferowanych usług ubezpieczeniowych.

Należy podkreślić, że zagadnienia poruszane w artykule mają i będą miały znaczenie dla bieżącego funkcjonowania zakładów ubezpieczeń. Zaproponowane ujęcie problemów badawczych uwzględnia nową perspektywę regulacyjną na tle aktualnych tendencji w tym zakresie. Autorzy żywią nadzieję, że przyczyni się również do poszerzenia wiedzy na temat nowych zagadnień dotyczących cyberbezpieczeństwa, które stanowi jedno z największych wyzwań współczesnego rynku finansowego.

Bibliografia

Allianz (2022), *Allianz Risk Barometer 2022*, https://www.agcs.allianz.com/news-and insights/reports/allianz-risk-barometer.html.

BBN (2015), *Doktryna bezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego.

CERT Polska (2022), *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego internetu,* NASK – Państwowy Instytut Badawczy.

Chochowski K. (2019), *Strategia cyberbezpieczeństwa jako przejaw polityki administracyjnej*, Zeszyty Naukowe Uniwersytetu Rzeszowskiego. Seria Prawnicza, 107/2019.

Cieślarczyk M. (2011), Pojęcie oraz typologie bezpieczeństwa i zagrożeń, w: B. Wiśniewski (red. nauk.), *Bezpieczeństwo w teorii badań naukowych*, Wydawnictwo Wyższej Szkoły Policji w Szczytnie.

Craigen D., Diakun-Thibault N., Purse R. (2014), Defining cybersecurity, *Technology Innovation Management Review*, 4(10), 13–21.

Eger J. (1981), The global phenomenon of teleinformatics. An introduction, *Cornell International Law Journal*, 14(2), 204–205.

EIOPA (2019), *Cyber Risk for Insurers – Challenges and Opportunities*, European Insurance and Occupational Pension Authority.

EIOPA (2020), *Guidelines on information and communication technology security and governance*, European Insurance and Occupational Pension Authority.

EIU (2022), *EIU Risk Outlook 2022. 10 scenarios that could impact global growth and inflation*, Economist Intelligence Unit, https://www.eiu.com/n/campaigns/risk-outlook-2022/.

Eurasia Group (2022), *Top Risks 2022*, https://www.eurasiagroup.net/files/upload/EurasiaGroup_TopRisks2022.pdf.

Gupta C.P., Goyal K.K. (2020), *Cybersecurity. A Self-Teaching Introduction*, Mercury Learning and Information.

Hale A., Baram M. (1998), Safety management, w: A. Halle, M. Baram (red. nauk.), *Safety Management. The Challenge of Change*, Pergamon Press.

Hoffmann T. (2018), *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Fundacja na rzecz Czystej Energii.

Kaczmarczyk B. (2013), Bezpieczeństwo i jego typologie, *BiTP,* 31(3), 20–21.

Koziej S. (2011), Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, *Bezpieczeństwo Narodowe*, II-2011(18), 19–41.

KPMG (2022), *Barometr cyberbezpieczeństwa. Ochrona cyfrowej tożsamości*, KPMG, https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2022/05/pl-raport-kpmg-w-polsce-barometr-cyberbezpieczenstwa-ochrona-cyfrowej-tozsamosci-secured.pdf.

Kuhlmann A. (1986), *Introduction to Safety Science*, Springer-Verlag.

Kulesza M., Filipowski P. (2022), Ryzyko wykorzystywania usług ICT w sektorze finansowym – omówienie wybranych wymogów projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA), *Monitor Prawniczy*, 15/2022, dodatek specjalny *Prawo Innowacji Finansowych (FinTech)*, 36–42.

Kulesza M., Racki T. (2022), *Ile DORA zmieni w podejściu zakładów ubezpieczeń do ICT ?*, https://maruta.pl/ile-dora-zmieni-w-podejsciu-zakladow-ubezpieczen-do-ict/.

Kuna M. (2020), *DORA – cyfrowa odporność operacyjna dla sektora finansowego*, Polska Izba Ubezpieczeń, https://piu.org.pl/blogpiu/dora-cyfrowa-odpornosc-operacyjna-dla-sektora-finansowego/.

Li Y., Guldenmund F. (2018), Safety management systems: a broad overview of the literature, *Safety Science*, 103, 94–123.

Mosteanu N. (2020), Artificial intelligence and cyber security – a shield against cyberattack as a risk business management tool. Case of European countries, *Quality – Access to Success*, 21(175), 148–156.

Mozur P., Sang-Hun Ch. (2017), North Korea's rising ambition seen in bid to breach global banks, *The New York Times*, 25 March, https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html.

Niebezpiecznik (2017), *Jak przeprowadzono atak na KNF i polskie banki oraz kto jeszcze był na celowniku przestępców?,* https://niebezpiecznik.pl/post/jak-przeprowadzono-atak-na-knf-i-polskie-banki-oraz-kto-jeszcze-byl-na-celowniku-przestepcow/.

Pelc P. (2021), Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce, *Cybersecurity and Law*, 5(1), 31–42.

Pałęga M., Wojtyto D., Salwierak M., Kulma W., Knapiński M. (2013), *Bezpieczeństwo teleinformatyczne jako element kompleksowej ochrony informacji*, Prace Naukowe Akademii im. J. Długosza w Częstochowie, 1.

Ruiz K. (2022), *DORA to rewolucja na rynku finansowym ? Być może, ale z innych powodów niż myślicie,* https://www.prawo.pl/biznes/dora-czyli-kontrola-instytucji-finansowych-i-dostawcow-uslug,517484.html.

Statista (2022), *Statista technology market outlook, Estimated cost of cybercrime globally 2016–2027.*

Walters R. (2015), *Cyber attacks on U.S. companies since November 2014*, The Heritage Foundation, 4487.

WEF (2022), *Global risk report 2022,* World Economic Forum, https://www.weforum.org/reports/global--risks-report-2022.

Węgrzyn Ł. (2021), Rozporządzenie ws. operacyjnej odporności cyfrowej sektora finansowego – uwagi na tle proponowanej regulacji, *Prawo Nowych Technologii*, 1/2021, 15–19.

Vecto (2020), *Raport 2020. Cyberbezpieczeństwo w polskich firmach,* https://vecto.pl/doc/Vecto--Cyberbezpieczenstwo-polskich-firm-2020.pdf.

Youchong L., Quingui L. (2021), A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments, *Energy Reports*, 7, 8176–8186.

ZBP (2020), *Postawy Polaków wobec cyberbezpieczeństwa*, Związek Banków Polskich.

Zouave E., Bruce M., Colde K., Jaitner M., Rodhe I., Gustafsson T. (2020), *Artificially Intelligent Cyberattacks*, Totalförsvarets forskningsinstitut FOI.

Regulacje prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014, dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dziennik Urzędowy Unii Europejskiej L 333/80.

Komisja Nadzoru Finansowego, Akty prawne rynku ubezpieczeń, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/regulacje_prawne/akty_prawne_rynku_ubezpieczen.

Komisja Nadzoru Finansowego, Rekomendacje i wytyczne, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne.

Komisja Nadzoru Finansowego, Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji, https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf.

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), Dziennik Urzędowy Unii Europejskiej L 333/1.

Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie działań zakładów ubezpieczeń i reasekuracji w zakresie cyberbezpieczeństwa z dnia 19 października 2022 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_ws_dzialan_zakladow_ubezpieczen_i_reasekuracji%20_w_zakresie_cyberbezpieczenstwa_79982.pdf.

Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, Dz. U. 2015 poz. 1844 z późn. zm.

Aneks

Tabela 1
Przewidywane koszty spowodowane cyberprzestępczością w latach 2016–2027 (estymacja)

Lata	Wartość (bln USD)	Dynamika r/r (%)
2016	0,61	–
2017	0,70	115
2018	0,86	123
2019	1,16	135
2020	2,95	254
2021	5,99	203
2022	8,44	141
2023	11,50	136
2024	14,57	127
2025	17,65	121
2026	20,74	118
2027	23,84	115
Suma	**109,01**	–

Źródło: opracowanie własne na podstawie: Statista (2022).

Tabela 2
Liczba cyberataków w Polsce w latach 1996–2021

Lata	Liczba	Dynamika r/r (%)	Lata	Liczba	Dynamika r/r (%)
1996	50	–	2009	1 292	72
1997	75	150	2010	674	52
1998	100	133	2011	605	90
1999	105	105	2012	1 082	179
2000	126	120	2013	1 219	113
2001	741	588	2014	1 282	105
2002	1 013	137	2015	1 456	114
2003	1 196	118	2016	1 926	132
2004	1 222	102	2017	3 182	165
2005	2 516	206	2018	3 739	118
2006	2 427	96	2019	6 484	173
2007	2 108	87	2020	10 420	161
2008	1 796	85	2021	29 483	283
Suma	**76 319**	–			

Źródło: opracowanie własne na podstawie: Statista (2022).

Tabela 3
Liczba i cele cyberataków w Polsce w latach 2019–2021 wg branż

Cel ataków (branża)	Liczba			Udział (w %)			Dynamika r/r (%)	
	2019	2020	2021	2019	2020	2021	2020	2021
Media	748	2 568	8 339	11,5	24,6	28,3	343	325
Handel hurtowy i detaliczny	624	1 437	5 125	9,6	13,8	17,4	230	357
Usługi pocztowe i kurierskie	49	500	4 338	0,8	4,8	14,7	1020	868
Sektor energetyczny	28	101	4 084	0,4	1,0	13,9	361	4044
Osoby fizyczne	1 212	959	2 464	18,7	9,2	8,4	79	257
Infrastruktura cyfrowa	550	1 016	1 606	8,5	9,8	5,4	185	158
Sektor bankowy	1 057	1 008	947	16,3	9,7	3,2	95	94
Infrastruktura rynków finansowych	500	1 283	563	7,7	12,3	1,9	257	44
Administracja publiczna	336	388	429	5,2	3,7	1,5	115	111
Produkcja	46	57	421	0,7	0,5	1,4	124	739
Hotele, restauracje, katering	9	19	295	0,1	0,2	1,0	211	1553
Transport	61	29	220	0,9	0,3	0,7	48	759
Służba zdrowia	53	112	150	0,8	1,1	0,5	211	134
Edukacja i wychowanie	62	71	142	1,0	0,7	0,5	115	200
Inne usługi	480	384	118	7,4	3,7	0,4	80	31
Budownictwo i zarządzanie nieruchomościami	31	29	89	0,5	0,3	0,3	94	307
Inne branże	578	379	68	8,9	3,6	0,2	66	18
Wodociągi	5	9	18	0,1	0,1	0,1	180	200
Logistyka i dystrybucja	19	27	18	0,3	0,3	0,1	142	67
Turystyka	8	9	15	0,1	0,1	0,1	113	167
Kultura i ochrona dziedzictwa narodowego	9	7	11	0,1	0,1	0,0	78	157
Wspólnoty i mniejszości religijne	3	8	6	0,0	0,1	0,0	267	75
Gospodarka odpadami	2	1	6	0,0	0,0	0,0	50	600
Izby gospodarcze i przemysłowe	0	3	4	0,0	0,0	0,0	–	133
Działalność ubezpieczeniowa	5	2	3	0,1	0,0	0,0	40	150
Rolnictwo	3	4	2	0,0	0,0	0,0	133	50
Kultura fizyczna	4	9	2	0,1	0,1	0,0	225	22
Rybołówstwo	2	1	0	0,0	0,0	0,0	50	0
Suma	6 484	10 420	29 483	100,0	100,0	100,0	161	283

Tabela 4
Liczba incydentów cyberbezpieczeństwa w Polsce w latach 2019–2021 według rodzajów

Pozycja	Liczba			Udział (w %)			Dynamika r/r (%)	
	2019	2020	2021	2019	2020	2021	2020	2021
Oszustwa	4 086	8 310	25 472	63,0	79,8	86,4	203	307
Złośliwe oprogramowanie	969	746	2 847	14,9	7,2	9,7	77	382
Obraźliwe i nielegalne treści	812	371	311	12,5	3,6	1,1	46	84
Wtargnięcia	160	317	247	2,5	3,0	0,8	198	78
Usługi wrażliwe	102	211	216	1,6	2,0	0,7	207	102
Dostępność zasobów	57	121	148	0,9	1,2	0,5	212	122
Próby włamań	77	174	127	1,2	1,7	0,4	226	73
Atak na bezpieczeństwo informacji	41	68	55	0,6	0,7	0,2	166	81
Zbieranie informacji	95	60	27	1,5	0,6	0,1	63	45
Inne	85	42	33	1,3	0,4	0,1	49	79
Suma	6 484	10 420	29 483	100,0	100,0	100,0	161	283

Źródło: opracowanie własne na podstawie: CERT Polska (2022, s. 23–24).

Tabela 5
Główne cyberzagrożenia dla organizacji w Polsce w 2022 r. według poziomu ryzyka

Pozycja / stopień zagrożenia	Poziom zagrożenia – odsetek wskazań przez ankietowanych						Suma (%)
	5	4	3	2	1	0	
Kradzieże danych przez pracowników	13	17	21	16	18	15	100
Zaawansowane trwałe zagrożenie	13	16	27	19	10	15	100
Phishing	11	21	28	20	10	10	100
Wycieki danych przez złośliwe oprogramowanie	8	23	29	17	16	7	100
Ataki *ransomware*	6	14	30	22	16	12	100
Wyciek danych spowodowany kradzieżą lub utratą nośników bądź urządzeń mobilnych	6	10	17	30	21	16	100
Ataki na urządzenia moblilne	3	9	17	23	27	21	100
Kradzież danych z powodu fizycznych naruszeń bezpieczeństwa	3	13	16	23	27	18	100
Ataki na sieci bezprzewodowe	2	9	26	24	19	20	100
Ataki *man-in-the-middle*	2	5	21	34	22	16	100
Ataki wykorzystujące błędy w aplikacjach	2	14	21	27	21	15	100
Ataki DoS/DDoS	1	7	23	30	14	25	100

Źródło: opracowanie własne na podstawie KPMG (2022, s. 11).

Cyber security of the Polish insurance sector in the context of national and EU regulations

Abstract

The security of transactions is one of the greatest challenges faced by the modern financial market. It has a direct impact on the shape of the offered products and is one of the most important elements determining their quality. Regulations regarding ICT security are one of the most important elements of the financial architecture at the level of individual countries and geographical areas. One of the key players in the financial market is the insurance companies analysed in this article.

The scope and content of regulations have been illustrated on the example of the regulations in force in the Polish insurance sector and the latest European Union regulations that entered into force at the beginning of 2023. The main purpose of this study is to analyse the current situation in the field of formal and legal regulations related to ICT security of insurance companies. The specific objectives are: quantitative analysis of market data regarding the ICT risk and the answer to the question of whether the new regulations will contribute to the increase in ICT security of the insurance sector.

The main objective and the specific objectives may in practice solve the problem faced by the management of insurance companies, looking for the most adequate methods of risk management in the area of procedures for anticipating, preventing and limiting the effects of cyber threats. This article focuses on those elements of the applicable regulations that are designed to meet the highest standards and will contribute to their further development in the coming years. The research methods used in the article are as follows: critical analysis of the literature, deduction as a method of theoretical reasoning, analysis of statistical data and induction to descriptive analysis.

The subject and purpose of the article have been illustrated against the background of the latest statistical data, applicable legal regulations, regulations of the Polish Financial Supervision Authority (KNF), which, according to their nature, are a clarification of already existing statutory provisions, and the latest regulations of the European Union. Detailed statutory requirements, KNF regulations and EU legal acts are the key element on which the safety and quality of the insurance services offered are built. The research and analyses show that in the face of the increase in cyber risk, the new Digital Operational Resilience Act (DORA), which entered at the beginning of 2023, will play a large role in increasing system security in the coming years. Implementation will result in adapting domestic regulations to new security standards by January 2025. The study also showed that both the current statutory requirements, KNF guidelines and new EU regulations are and will be the basis for maintaining the security and quality of financial services offered. It should be emphasized that the issues discussed in the article have, and in the future will also have, a strict practical application in the current functioning of insurance companies.

The issues raised in the article have practical application, because in the current functioning of financial institutions and insurance companies, all applicable regulations must be observed and respected. The approach proposed in the article presents the discussed issues from a new, so far rarely discussed regulatory perspective.

Keywords: security, cyberattacks, ICT, insurance companies, legal acts, guidelines and recommendations, KNF