Acta Iuris Stetinensis

2023, nr 2 (vol. 43), 107–122
ISSN (print) 2083-4373 ISSN (online) 2545-3181
DOI: 10.18276/ais.2023.43-06

Dominika Skoczylas
dr
Uniwersytet Szczeciński
e-mail: dominika.skoczylas@usz.edu.pl
ORCID: 0000-0003-1231-8078

Cyberbezpieczeństwo sektora bankowego i infrastruktury rynków finansowych

Streszczenie

W artykule poruszono problematykę cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych. Rozważania w tym zakresie przeprowadzono na podstawie analizy przepisów ustawy o krajowym systemie cyberbezpieczeństwa. Ponadto uwzględniono aktualne zasady cyberbezpieczeństwa w kontekście zadań Komisji Nadzoru Finansowego. W pracy wykorzystano metodę dogmatycznoprawną.

Celem artykułu jest scharakteryzowanie zagrożeń występujących w sektorze bankowym i infrastruktury rynków finansowych w związku ze świadczeniem tzw. e-usług w cyberprzestrzeni. Przedmiotem rozważań jest ponadto przedstawienie i ocena aktualnych zasad cyberbezpieczeństwa oraz zadań Komisji Nadzoru Finansowego (organu właściwego do spraw cyberbezpieczeństwa). Kluczowym aspektem jest również wskazanie działań podejmowanych przez właściwy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT KNF), szczególnie w kontekście klasyfikacji oraz obsługi incydentów sieciowych. Analiza tematu pozwoli odpowiedzieć na pytanie: jakie kwestie należy wziąć pod uwagę przy wdrożeniu polityki cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych.

Autorka pracy ustaliła, że współczesny wymiar bezpieczeństwa finansowego państwa to również wymiar bezpieczeństwa e-finansów. Biorąc pod uwagę powyższe, kluczowym aspektem jest wdrożenie optymalnej polityki cyberbezpieczeństwa, ale również rozwój umiejętności (kompetencji) cyfrowych aktorów rynku finansowego.

Słowa kluczowe: cyberbezpieczeństwo, cyberzagrożenia, Komisja Nadzoru Finansowego, sektor bankowy i infrastruktury rynków finansowych, usługi kluczowe

Wprowadzenie

Nowoczesne technologie informacyjno-komunikacyjne (dalej: ICT) są podstawowym warunkiem rozwoju organizacji oraz świadczenia usług na odległość. Co więcej, korzystanie z nowoczesnych narzędzi teleinformatycznych dotyczy zarówno sektora usług publicznych, jak i usług prywatnych. Współcześnie wspólnym mianownikiem dla bezpieczeństwa publicznego i jednostkowego jest cyberbezpieczeństwo. Ukształtowanie nowego sposobu postępowania organów administracji publicznej, tj. działania w cyberprzestrzeni, pozwala na określenie dwóch podstawowych komponentów cyberbezpieczeństwa. Pierwszym z nich jest ochrona infrastruktury krytycznej (zapewnienie ciągłości świadczenia e-usług), drugim osiągnięcie celów użyteczności publicznej, przy zachowaniu prywatności i bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych[1]. Tak przedstawione determinanty cyberbezpieczeństwa są jednak zbyt dużym uproszczeniem, w rzeczywistości bowiem wskazany termin wymaga większej konkretyzacji odnośnie do funkcji, roli i zadań organów właściwych do spraw cyberbezpieczeństwa oraz potencjalnych zagrożeń cyberprzestrzeni.

Zważywszy na liczne incydenty występujące w szczególności w sektorze usług kluczowych i usług cyfrowych, *sine qua non* nieprzerwanego świadczenia usług jest wdrożenie kompleksowej polityki cyberbezpieczeństwa. Należałoby zatem ocenić pozytywnie zaliczenie bezpieczeństwa w cyberprzestrzeni do tzw. globalnych dóbr publicznych oraz wprowadzenie do katalogu dyscyplin naukowych – nauki o bezpieczeństwie w cyberprzestrzeni (tzw. securitologia)[2]. W kontekście podejmowanych rozważań istotne jest sprecyzowanie kluczowych czynników mających wpływ na wypracowanie zasad cyberbezpieczeństwa. Do pierwszej grupy należy rozwój oraz popularyzacja ICT w usługach. Mówiąc o nich, należy wskazać na rozbudowany, a jednocześnie różnorodny katalog e-usług, takich jak: handel elektroniczny, *e-learning* czy *cloud computing*. Ze względu na aspekt użyteczności publicznej pryncypialne znaczenie przypisuje się funkcjonowaniu elektronicznej administracji oraz świadczeniu tzw. usług kluczowych. W odniesieniu do e-administracji

1 T. Hoffmann, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018, s. 20.

2 Zob. C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 35–37.

M. Błażewski podkreśla, że „środki komunikacji elektronicznej służą ułatwieniu przekazywania informacji m.in. wewnątrz administracji publicznej oraz pomiędzy podmiotami prywatnymi a organami administracji publicznej i podmiotami administrującymi”[3]. Z kolei A. Monarcha-Matlak wskazuje na istotną rolę prawa komunikacji elektronicznej, które „powoduje, że powstaje nowa jakość działania, nowy sposób pracy oraz nowe struktury administracyjne”[4]. Z powyższego wynika, że na organach administracji publicznej ciąży obowiązek ciągłego doskonalenia procesów związanych z zarządzaniem organizacją, lecz także budowanie bezpiecznego środowiska e-usług dla użytkowników. Podobne działania powinny też podjąć podmioty realizujące usługi kluczowe w cyberprzestrzeni.

W celu usystematyzowania, podkreślenia wymagają trzy podstawowe determinanty, pozwalające na wdrożenie skutecznych zasad cyberbezpieczeństwa, tj. prawne, społeczne i technologiczne. Pierwsze z nich nie budzą większych wątpliwości, aczkolwiek podstawy prawne cyberbezpieczeństwa powinny odzwierciedlać przyjęte przez społeczność międzynarodową rozwiązania oraz uwzględniać aktualne zagrożenia prawidłowego funkcjonowania cyberprzestrzeni. Wyzwaniem są potrzeby społeczeństwa informacyjnego, dla którego dostęp do informacji i ich przetwarzanie (współcześnie również za pomocą środków komunikacji elektronicznej) jest najwyższą wartością, dobrem szczególnego rodzaju[5]. Kluczowa jest w tym przypadku zasada równego dostępu do usług. Spoiwem aspektów prawnych i społecznych są nowe technologie, aspekty cyfryzacji, takie jak interoperacyjność, transgraniczność, a nawet sztuczna inteligencja[6]. Szczególnie skomplikowane wydaje się zapewnienie cyberbezpieczeństwa świadczenia usług kluczowych,

3 M. Błażewski, *Środki komunikacji elektronicznej w prawie zamówień publicznych*, „Research Papers of Wrocław University of Economics” 2017, nr 497, s. 272, DOI: 10.15611/pn.2017.497.19 (dostęp 1.06.2022).

4 A. Monarcha-Matlak, *Komunikacja elektroniczna, prawo komunikacji elektronicznej, Europejski kodeks łączności elektronicznej i ich wpływ na rozwój jurysdykcji administracyjnej*, w: M. Szewczyk, L. Staniszewska, M. Kruś (red.), *Kierunki rozwoju jurysdykcji administracyjnej*, Warszawa 2022, s. 270.

5 Zob. E. Żywucka-Kozłowska, R. Dziembowski, *Społeczeństwo informacyjne w perspektywie wybranych aktów prawnych Unii Europejskiej*, „Media – Kultura – Komunikacja Społeczna” 2021, nr 3 (16), s. 77–78, DOI: 10.31648/mkks.6620 (dostęp 1.06.2022).

6 Zob. D. Skoczylas, *Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku*, w: M. Staniszewski, H.E. Kretek (red.), *Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonalenia warsztatu naukowca*, Gliwice 2021, s. 234–237.

do których ustawodawca zaliczył m.in. sektor bankowy i infrastruktury rynków finansowych[7].

Prawidłowe, efektywne, a przede wszystkim bezpieczne funkcjonowanie tego sektora to niezbędny warunek rozwoju społeczno-gospodarczego państwa. Cyfryzacja dotyczy sektora bankowego w znaczącym stopniu (co niestety wiąże się również ze wzrostem skali zagrożeń). Celem artykułu jest zatem scharakteryzowanie zagrożeń występujących w sektorze bankowym i infrastruktury rynków finansowych w związku ze świadczeniem tzw. e-usług w cyberprzestrzeni. Przedmiotem rozważań jest przedstawienie i ocena aktualnych zasad cyberbezpieczeństwa oraz zadań Komisji Nadzoru Finansowego (organu właściwego do spraw cyberbezpieczeństwa dla operatorów usług kluczowych z sektora bankowego i infrastruktury rynków finansowych[8]), a także wskazanie działań podejmowanych przez właściwy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT KNF). Analiza tematu pozwoli odpowiedzieć na pytanie: jakie kwestie należy wziąć pod uwagę przy wdrożeniu polityki cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych?

Cyberbezpieczeństwo a cyberzagrożenia sektora bankowego i infrastruktury rynków finansowych. Cyberbezpieczeństwo usług kluczowych

Środki komunikacji elektronicznej są obecne w wielu dziedzinach życia publicznego. Nie oznacza to jednak, że narzędzia teleinformatyczne całkowicie zastąpiły tradycyjne formy działania. Stały się natomiast istotnym elementem zmian w zakresie świadczenia usług oraz funkcjonowania organizacji. Pozytywnym aspektem jest to, że ICT tworzą nowego rodzaju relacje pomiędzy usługodawcą a usługobiorcą, organem a obywatelem, ponadto modernizują sposób świadczenia usług i realizacji zadań publicznych[9]. Wdrożenie środków komunikacji elektronicznej wymaga zapewnienia cyberbezpieczeństwa zarówno w aspekcie podmiotowym (użytkowników e-usług i podmiotów odpowiedzialnych za ich świadczenie), jak i przedmiotowym (nieprzerwany dostęp do usługi o wysokiej jakości i ochrona przed cyberzagrożeniami). Niemniej jednak należy wskazać kilka czynników mających

7 Zob. Załącznik nr 1 Sektory i podsektory oraz rodzaje podmiotów do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022 r., poz. 655), dalej: u.k.s.c.

8 Zob. art. 41 pkt 4 u.k.s.c.

9 K. Drgas, *Przesłanki wdrażania cyfryzacji jednostek samorządu lokalnego finansowanej ze środków unijnych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2019, nr 81 (1), s. 194–195, DOI: 10.14746/rpeis.2019.81.1.13 (dostęp 11.06.2022).

kluczowe znaczenie dla zapewnienia cyberbezpieczeństwa. Na ostateczny kształt polityki cyberbezpieczeństwa mają wpływ warunki społeczne (potrzeby społeczeństwa informacyjnego, e-użytkowników), organizacyjne (związane z e-zarządzaniem, popularyzacją e-usług w sektorze prywatnym i publicznym), kompetencje cyfrowe usługobiorców i usługodawców (bądź ich brak), rodzaj i częstotliwość występujących cyberzagrożeń, a także kwestie technologiczne.

Choć cyberbezpieczeństwo nie jest uregulowane konstytucyjnie, należy przyjąć, że podlega ono szczególnej ochronie organów władzy publicznej. Jest niewątpliwie jednym z rodzajów bezpieczeństwa[10], rozumianego najczęściej jako bezpieczeństwo Internetu, bezpieczeństwo komputerowe czy bezpieczeństwo sieci. W przypadku zmiany konstytucji optymalnym zabiegiem byłoby wprowadzanie (choćby w minimalnym zakresie) kwestii odnoszących się do cyberbezpieczeństwa, które miałoby kluczowe znaczenie w kontekście określenia zasad bezpieczeństwa cybernetycznego w danym sektorze usług publicznych. W świetle powyżej przedstawionych rozważań, być może klasyfikacja cyberbezpieczeństwa jako pojęcia konstytucyjnego umożliwiłaby uzyskanie jednolitej definicji tego terminu. Istotny problem w tym zakresie zauważa G. Szpor. Wskazuje przede wszystkim na niespójności terminologiczne w zakresie używania pojęcia „cyberbezpieczeństwo" w ustawie o krajowym systemie cyberbezpieczeństwa[11] i w tzw. akcie o cyberbezpieczeństwie[12]. Zauważyć przy tym należy, że ze względu na prawidłowe i efektywne funkcjonowanie usług kluczowych czy prowadzenie działalności cyfrowej niezbędne jest „wyraźne rozstrzygnięcie czy cyberbezpieczeństwo to odporność czy działania niezbędne do

10 Art. 5 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483 ze zm.) dalej: Konstytucja RP stanowi, że Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju.

11 Zgodnie z art. 2 pkt 4 u.k.s.c, cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

12 Art. 2 pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L nr 151 z dnia 17.04.2019 r., s. 15) stanowi, że: cyberbezpieczeństwo oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. Z kolei za cyberzagrożenie uznaje się wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób (art. 2 pkt 8 aktu o cyberbezpieczeństwie).

ochrony przed cyberzagrożeniami[13]". Tym samym bez przesądzania o tym, która z definicji jest ważniejsza, ustawodawca w przypadku nowelizacji u.k.s.c mógłby zastanowić się nad uzupełnieniem definicji cyberbezpieczeństwa o kwestie związane z podmiotową i przedmiotową płaszczyzną ochrony przed cyberzagrożeniami, w szczególności gdy mowa o cyberbezpieczeństwie usług kluczowych. Do tej grupy należy sektor bankowy i infrastruktury rynków finansowych.

Sektor bankowy i infrastruktury rynków finansowych został umieszczony w wykazie tzw. usług kluczowych, za które uznaje się te posiadające wyjątkową, kluczową rolę dla utrzymania krytycznej działalności społecznej lub gospodarczej[14]. Współcześnie trudno sobie wyobrazić, aby sektor finansowy funkcjonował bez nowych technologii informacyjno-komunikacyjnych. Wiedząc, że tworzy go wiele podmiotów, m.in.: instytucje kredytowe, bank krajowy, oddziały banków zagranicznych, oddziały instytucji kredytowych, spółdzielcze kasy oszczędnościowo-kredytowe czy podmioty prowadzące rynek regulowany[15], koniecznym zabiegiem wydaje się utworzenie skutecznej, ale jednocześnie efektywnej polityki cyberbezpieczeństwa. Oczywiście, mając na uwadze różnorodność struktur wewnętrznych oraz częstotliwość występowania incydentów, strategia cyberbezpieczeństwa powinna być dostosowana do potrzeb organizacji. Zresztą podmioty odpowiedzialne za przygotowanie polityki cyberbezpieczeństwa w tym sektorze oprócz celu głównego (ograniczenie występowania cyberzagrożeń i zapewnienie ciągłości świadczenia usług), powinny zapewnić „zrównoważony wzrost gospodarczy oraz stabilność systemu finansowego"[16]. Na szczególną uwagę zasługują regulacje związane przede wszystkim z określeniem statusu i zadań operatorów usług kluczowych w odniesieniu do incydentów, czyli zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo (art. 2 pkt 5 u.k.s.c.) oraz innego rodzaju cyberzagrożeń (głównie cyberprzestępstw). Podstawową przesłanką uznania podmiotu za operatora usługi kluczowej jest świadczenie tego typu usługi za pomocą systemów informacyjnych. Dodatkową determinantą, która uzasadnia zakres obowiązków operatorów usług kluczowych, jest możliwość wystąpienia incydentu. Ustawodawca dokonuje zresztą

13 G. Szpor, *Nowelizacja siatki pojęciowej cyberbezpieczeństwa*, „Monitor Prawniczy" 2020, nr 22, s. 1192.

14 Zob. art. 2 pkt 16 u.k.s.c.

15 Zob. Załącznik nr 1 do u.k.s.c. Sektory i podsektory oraz rodzaje podmiotów.

16 P. Klepacka, E. Kowalewska, *Instrumenty polityki pieniężnej w działalności Narodowego Banku Polskiego*, w: W. Bożek, E. Kowalewska (red.), *Bank i pieniądz w Polsce i na świecie*, Szczecin 2017, s. 191.

ich klasyfikacji[17] i słusznie wskazuje na podstawowe problemy związane z obniżeniem jakości lub przerwaniem ciągłości świadczenia usługi kluczowej czy wyrządzeniem znacznej szkody.

De lege lata w przepisach wyznaczono wprost obowiązki związane z tzw. obsługą incydentu (art. 2 pkt 10 u.k.s.c.) czy szacowaniem ryzyka (art. 2 pkt 13 u.k.s.c). Przedmiotowe obowiązki polegają na zarządzaniu bezpieczeństwem informacji. Można je podzielić na trzy podstawowe grupy. Do pierwszej z nich należą zadania związane z szacowaniem ryzyka wystąpienia incydentu (potencjalnych okoliczności sprzyjających powstaniu zagrożenia). Drugą grupą są odpowiednie środki techniczne i organizacyjne służące zapewnieniu bezpieczeństwa i ciągłości dostawy usług. Ostatnią grupę stanowią działania następcze, na które składają się czynności zarządzania incydentami i działania polegające na przywróceniu świadczenia usług. Pozytywnie ocenić należy także działania informacyjne dotyczące zapewnienia dostępu do informacji na temat cyberzagrożeń dla użytkownika usługi kluczowej, m.in. za pomocą informacji o incydentach na stronie internetowej usługodawcy[18].

Niestety, zważywszy na liczbę i różnorodność cyberzagrożeń, a także wzrost kompetencji cyfrowych (zaawansowanie technologiczne) cyberprzestępców, działania podejmowane wyłącznie przez operatorów usług kluczowych nie byłyby wystarczające. Ustawodawca wprowadził dlatego inne podmioty odpowiedzialne (i wspierające) za zapewnienie cyberbezpieczeństwa, m.in. organ właściwy do spraw cyberbezpieczeństwa, sektorowe zespoły cyberbezpieczeństwa czy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego. W tym miejscu należy odnotować, że w przypadku sektora bankowego i infrastruktury rynków finansowych podmioty odpowiedzialne za zagwarantowanie cyberbezpieczeństwa stoją przed bardzo trudnym zadaniem. Wynika to z tego, że sektor finansowy jest częstym celem cyberataków, które przyjmują różne postaci. Obok klasycznych cyberzagrożeń, takich jak: wirusy, robaki, złośliwe oprogramowanie (*malware*), bomby logiczne, konie trojańskie[19], spam, pojawiają się coraz bardziej zaawansowane metody nieuprawnionego dostępu do sieci. Szczególnie niebezpieczne są: *phishing* (podszywanie się w celu wyłudzenia informacji), *pharming* (przekierowanie na niewłaściwy serwer, stronę) czy szpiegostwo internetowe (tzw. *spyware*, stosowanie

17 Incydentami tymi są: incydent krytyczny (art. 2 pkt 6 u.k.s.c.), incydent poważny (art. 2 pkt 7 u.k.s.c.), incydent istotny (art. 2 pkt 8 u.k.s.c.), incydent w podmiocie publicznym (art. 2 pkt 9 u.k.s.c.).

18 F. Krzyżankiewicz, *Ustawa o krajowym systemie cyberbezpieczeństwa. Identyfikacja i rejestracja operatorów usług kluczowych*, „Informacja w administracji publicznej" 2019, nr 1, s. 72.

19 T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15 (8), s. 15.

programów szpiegowskich)[20]. Skutkiem pojawienia się powyższych cyberzagrożeń jest nie tylko przerwanie ciągłości świadczenia usługi kluczowej, lecz także utrata danych osobowych i środków finansowych zgromadzonych na rachunkach. K. Chałubińska-Jentkiewicz podkreśla, że to właśnie „dane udostępniane w sieci teleinformatycznej mogą jednak stanowić źródło zagrożeń dla bezpieczeństwa informacyjnego[21]". Z kolei T. Hoffmann wskazuje, że banki działające jako instytucje zaufania publicznego powinny prowadzić skuteczną politykę cyberbezpieczeństwa w celu zapewnienia ciągłości świadczenia usług i ochrony danych osobowych swoich klientów. Należy podkreślić, że zapewnienie jednolitego bezpieczeństwa w skali całego kraju dla całego sektora bankowego i infrastruktury rynków finansowych utrudnia choć w minimalnym zakresie sposób zarządzania bezpieczeństwem cyberprzestrzeni oraz zakres świadczonych usług[22]. W obliczu licznych cyberzagrożeń warto zatem scharakteryzować zadania właściwych podmiotów odpowiedzialnych za politykę cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych, w szczególności Komisji Nadzoru Finansowego oraz sektorowego zespołu cyberbezpieczeństwa.

Zadania Komisji Nadzoru Finansowego oraz Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT KNF)

Z aprobatą należy odnieść się do umieszczenia sektora bankowego i infrastruktury rynków finansowych w wykazie usług kluczowych. Warto przy tym zaznaczyć, że zapewnienie cyberbezpieczeństwa w tym sektorze ma wpływ na rozwój społeczno-gospodarczy w kilku aspektach, tj. funkcjonowania instytucji finansowych (ciągłość świadczenia usług), ochrony użytkowników indywidualnych (bezpieczeństwo obrotu gotówkowego i bezgotówkowego) oraz płynności finansowej państwa (oddziaływanie na gospodarkę). Jeżeli chodzi o świadczenie e-usług w sektorze finansowym, kluczowe jest rejestrowanie czynności w e-systemach, co pozwala na „identyfikację rodzaju przetwarzanych informacji, określenie podstawy prawnej

20 K. Bartczak, M. Bodych-Biernacka, *Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście stosowania cyfrowych platform technologicznych w Polsce i UE*, „Przegląd Organizacji" 2021, nr 3 (974), s. 42–43, DOI: 10.33141/po.2021.3.05 (dostęp 20.06.2022).

21 K. Chałubińska-Jentkiewicz, *Bezpieczeństwo prawne danych osobowych w nowych warunkach cyfrowych*, „Zeszyty Naukowe Katolickiego Uniwersytetu Lubelskiego Jana Pawła II" 2018, nr 61 (1), s. 186, DOI: 10.31743/zn.2018.61.1.179-196 (dostęp 20.06.2022).

22 T. Hoffmann, *Wybrane...*, s. 87–88.

ich wykorzystywania, w tym polityki bezpieczeństwa i oceny jej skutków"[23]. Przedmiotowe działania obejmują zarówno politykę cyberbezpieczeństwa w znaczeniu makro (usług), jak i mikro (indywidualnych użytkowników). Tym bardziej, że na cyberatak mogą być narażone różnego rodzaju transakcje internetowe czy mobilne, dokonywane przy użyciu kart płatniczych czy za pomocą bliku.

W związku z powyższym należy określić tzw. obszary cyberbezpieczeństwa w sektorze finansowym. Rozważania zawarte w pracy wskazują, że istotną kwestią jest zapewnienie cyberbezpieczeństwa danych przetwarzanych w systemach informatycznych. W tym zakresie polityka cyberbezpieczeństwa powinna uwzględniać zasady określone w rozporządzeniu o ochronie danych osobowych[24] oraz uzupełniająco treść ustawy o ochronie danych osobowych[25]. Zachowanie integralności, dostępności i poufności danych jest jednym z elementów mających wpływ na zapewnienie bezpieczeństwa transakcji płatniczych. Jednocześnie polityka cyberbezpieczeństwa musi również zawierać klarowny opis obsługi incydentów, czynności podejmowanych w celu ochrony infrastruktury krytycznej, serwerów i systemów bankowych oraz zachowania ciągłości połączeń (nieprzerwanego świadczenia e-usług). T. Terlikowski wskazuje wprost, że

> problem bezpieczeństwa w cyberprzestrzeni wynika z faktu jej znaczenia dla funkcjonowania państwa (…) współczesnego społeczeństwa, administracji rządowej, samorządowej, gospodarczej i wszystkich innych uczestników życia społeczno-polityczno-gospodarczego[26].

Cyberryzyko w obszarze finansowym związane jest nie tylko ze stratą o *stricte* finansowym charakterze czy też zawieszeniem prawidłowego funkcjonowania infrastruktury (odmowa wykonania usługi). Banki i instytucje finansowe jako podmioty tzw. zaufania publicznego w przypadku wystąpienia cyberzagrożenia narażone są również na tzw. straty marketingowe, do których należą m.in.: „utrata przychodów wynikających z wyłączeń systemu, koszty utraty klientów i pozyskiwania nowych,

23 D. Skoczylas, *Przetwarzanie danych osobowych a prawo do bycia zapomnianym i prawo do przenoszenia danych na gruncie RODO*, „Acta Iuris Stetinensis" 2018, nr 4 (24), s. 98, DOI: 10.18276/ais.2018.24-04 (dostęp 20.06.2022).

24 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L nr 119 z dnia 4.05.2016 r., s. 1).

25 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781).

26 T. Terlikowski, *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)*, „Zeszyty Naukowe Szkoły Głównej Służby Pożarniczej" 2019, nr 71/3, s. 84.

utrata reputacji i zmniejszenie wartości firmy"[27]. W konkluzji przedstawionych stwierdzeń można odnieść wrażenie, że w tak kluczowym sektorze niezbędna jest współpraca właściwych podmiotów w celu maksymalizacji cyberbezpieczeństwa świadczenia e-usług. W istocie ustawodawca oceniając ryzyko wystąpienia cyberzagrożenia jako wysokie i uwzględniając różnorodność rynku finansowego w skali makro (usługi bankowe, płatnicze, kapitałowe, ubezpieczeniowe czy emerytalne), określił funkcje i zadania właściwych podmiotów odpowiedzialnych za cyberbezpieczeństwo w tym sektorze.

Organem właściwym do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych jest Komisja Nadzoru Finansowego – dalej: KNF (art. 41 pkt 4 u.k.s.c). Rola KNF jako podmiotu sprawującego nadzór nad sektorem bankowym jest istotna zarówno w kontekście „dbałości o uczestników rynku", jak i „podejmowania działań służących prawidłowemu funkcjonowaniu rynku finansowego oraz działań mających na celu rozwój rynku finansowego i jego konkurencyjności"[28]. Ogólne obowiązki KNF jako organu właściwego do spraw cyberbezpieczeństwa *de lege lata* wskazano m.in. w art. 42 ust. 1 u.k.s.c. Można stąd wywnioskować trzy podstawowe kategorie zadań obejmujące: prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania (bądź nieuznania) ich za operatora usługi kluczowej (w tym wydawania decyzji w zakresie uznania, stwierdzenia wygaśnięcia takiego statusu), kontrole operatorów usług kluczowych i dostawców usług cyfrowych (oraz bieżący monitoring stosowania przepisów ustawy), a także współpracy w zakresie cyberbezpieczeństwa z m.in.: ministrem właściwym ds. informatyzacji, z zespołami CSIRT (NASK, GOV, MON)[29], organami państw członkowskich Unii Europejskiej. Wyzwania stojące przed KNF odnoszą się do zapewnienia cyberbezpieczeństwa transakcji w skali makro, tj. przede wszystkim handlu elektronicznego i gospodarki elektronicznej. Istotnie, należy stworzyć warunki niezbędne dla bezpieczeństwa dostawców usług

27 A. Krawczyk-Jezierska, *Koszty instytucji finansowych w świetle zagrożeń cybernetycznych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 8 (854), s. 29.

28 P. Pisarewicz, E. Kowalewska, *Wybrane zagadnienia regulacji prawa bankowego i nadzoru nad rynkiem finansowym w kontekście praktyki ochrony klientów sektora bankowego*, „Zarządzanie i Finanse. Journal of Management and Finance" 2017, nr 2/1, s. 38.

29 CSIRT GOV to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego (art. 2 pkt 1 u.k.s.c.), CSIRT MON to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej (art. 2 pkt 2 u.k.s.c.), CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (art. 2 pkt 3 u.k.s.c.).

(np. banków, instytucji pieniądza elektronicznego czy instytucji kredytowych) oraz użytkowników usług (np. posiadaczy kart płatniczych, rachunków bieżących, kredytobiorców)[30].

Potrzeba podjęcia działań związanych z zapewnieniem cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych stała się impulsem do powstania sektorowego zespołu cyberbezpieczeństwa znanego pod nazwą Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego (dalej: CSIRT KNF). CSIRT KNF ściśle współpracuje z innymi krajowymi zespołami CSIRT. Do jego zadań należy również koordynacja działań i wsparcie czynności wykonywanych przez operatorów usług kluczowych, dotyczących w szczególności obsługi incydentów poważnych, występujących w podmiotach rynku finansowego świadczących usługi kluczowe. Ponadto CSIRT KNF zajmuje się także analizą incydentów i potencjalnych zagrożeń cyberbezpieczeństwa[31].

Kolejny moduł aktywności w zakresie cyberbezpieczeństwa dotyczy funkcjonowania Departamentu Cyberbezpieczeństwa Urzędu KNF (dalej: DCB). DCB powstało w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa Urzędu KNF oraz wykonywania zadań przewidzianych dla podmiotu publicznego oraz organu właściwego. Zajmuje się kwestiami analitycznymi, tj. opracowuje kryteria oceny i procedury kontrolne dotyczące podmiotów nadzorowanych, i kontrolnymi, tj. planuje i wykonuje czynności kontrolne w zakresie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego (czego skutkiem są m.in raporty czy zalecenia pokontrolne). Odpowiada również za przygotowywanie projektów decyzji Komisji, opracowuje dobre praktyki oraz rekomendacje dla rynku finansowego, zarządza incydentami w obszarze cyberbezpieczeństwa, współpracuje m.in. z ministrem właściwym ds. informatyzacji oraz z zespołami CSIRT [32]. Rozbudowanie schematu organizacyjnego Urzędu KNF, tj. pojawienie się Departamentu Cyberbezpieczeństwa, należy ocenić pozytywnie. Dodatkowa komórka zajmująca się cyberbezpieczeństwem pozwoli odciążyć (czy też wesprzeć) działania KNF-u w przedmiocie zapewnienia wysokiego poziomu bezpieczeństwa sektora bankowego i infrastruktury rynków finansowych. Podejmowane przez nią działania są szczególnie istotne w kontekście tzw. czynności prewencyjnych, polegających

30 P. Widawski, *Cyberbezpieczeństwo w usługach płatniczych*, w: C. Banasiński (red.), *Cyberbezpieczeństwo…*, s. 340.

31 Komisja Nadzoru Finansowego, *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego*, www.knf.gov.pl/dla_rynku/CSIRT_KNF (dostęp 21.06.2022). Por. art. 44 u.k.s.c.

32 Komisja Nadzoru Finansowego, *Departament Cyberbezpieczeństwa (DCB)*, www.knf.gov.pl/o_nas/urzad_komisji/dane_teleadresowe_struktura?articleId=65223&p_id=18 (dostęp 21.06.2022).

na opracowaniu dobrych praktyk oraz rekomendacji dla rynku finansowego. Warto wspomnieć, że działania KNF, CSIRT KNF oraz DCB powinny poprawić jakość świadczenia usług „pod względem interoperacyjności sieci na poziomie transgranicznym”[33], dlatego polityka cyberbezpieczeństwa stanowi nieodzowny element funkcjonowania tego sektora.

Na kanwie przedstawionych rozważań należy odnieść się do wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego[34]. Rozporządzenie konstruuje jednolite zasady bezpieczeństwa sieci i systemów operacyjnych wykorzystywanych w procesach biznesowych przez podmioty finansowe (m.in.: instytucje płatnicze, instytucje pieniądza elektronicznego czy firmy inwestycyjne). DORA podkreśla podstawowe zadania związane z zapewnieniem cyberbezpieczeństwa rynku finansowego. Odnoszą się one do zarządzania ryzykiem związanym z ICT, klasyfikacji i zgłaszania incydentów, testowania operacyjnej odporności cyfrowej, nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, wymiany informacji o cyberzagrożeniach[35]. Harmonizacja przepisów w tym zakresie w założeniu pozwoli osiągnąć wysoki wspólny poziom operacyjnej odporności cyfrowej, ograniczyć ryzyko zakłócenia świadczenia usługi kluczowej (ochrona usługodawców i usługobiorców), tym samym umożliwi wzrost konkurencyjności na rynku finansowym. Powyższe nie zmienia jednak tego, że oprócz regulacji prawnych istotne znaczenie w kontekście poprawy cyberbezpieczeństwa mają kompetencje cyfrowe aktorów cyberprzestrzeni. Należy zgodzić się ze stanowiskiem wyrażonym przez R. Piterę, że „za poprawę bezpieczeństwa odpowiada sam użytkownik, który jest tym elementem, który obecnie bywa najczęściej narażony na potencjalny atak ze strony hakerów”[36]. Jednocześnie warto zaznaczyć, że umiejętności cyfrowe nie są wystarczającą determinantą w walce z cyberzagrożeniami. Niezbędne warunki cyberbezpieczeństwa obejmują przede wszystkim kwestie technologiczne i prawne.

33 D. Skoczylas, *The Act on the National Cybersecurity System and Other Legal Regulations in the Context of Ensuring State Cybersecurity. Selected Issues*, „Roczniki Nauk Prawnych” 2020, t. XXX, nr 2, s. 96, DOI: 10.18290/rnp20302-7 (dostęp 21.06.2022).

34 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 24 września 2020 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 (COM(2020) 595 final), dalej: DORA.

35 Zob. art. 1 DORA.

36 R. Pitera, *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności” 2017, nr 2 (4), s. 190.

Wnioski

Reasumując, sektor bankowy i infrastruktury rynków finansowych należy do tzw. usług kluczowych. Zapewnienie niezakłóconego funkcjonowania rynku finansowego sprzyja nie tylko konkurencyjności usług, lecz także ma kluczową rolę dla utrzymania krytycznej działalności społecznej i gospodarczej. Niewątpliwie polityka pieniężna państwa ma fundamentalne znaczenie w kontekście rozwoju społeczno-gospodarczego. Zważywszy na liczne i różnorodne zagrożenia związane z użytkowaniem cyberprzestrzeni (cyberzagrożenia), konieczne jest stworzenie optymalnych, a jednocześnie skutecznych ram bezpiecznego świadczenia e-usług, zawartych w tzw. polityce cyberbezpieczeństwa.

Przy wdrożeniu polityki cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych należy wziąć pod uwagę kilka istotnych czynników. Przede wszystkim analizy wymaga kwestia istniejących i potencjalnych cyberzagrożeń, skali ich występowania, a także szkód, które mogą spowodować. Taka klasyfikacja pomoże m.in. przyjąć ogólne zasady postępowania w odniesieniu do analizy ryzyka oraz obsługi incydentów. Nie bez znaczenia są także zadania podmiotów odpowiedzialnych za cyberbezpieczeństwo rynku finansowego. Z aprobatą należy odnieść się do tego, że w przypadku sektora bankowego i infrastruktury rynków finansowych oprócz wskazania zadań organu właściwego do spraw cyberbezpieczeństwa, tj. Komisji Nadzoru Finansowego, wyodrębniono i przypisano liczne obowiązki Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego (CSIRT KNF). W tym miejscu warto wspomnieć o funkcjonowaniu Departamentu Cyberbezpieczeństwa Urzędu KNF, którego celem jest zapewnienie wysokiego poziomu cyberbezpieczeństwa Urzędu KNF oraz wykonywanie zadań przewidzianych dla podmiotu publicznego oraz organu właściwego. Mając na uwadze powyższe, można stwierdzić, że polityka cyberbezpieczeństwa powinna opierać się na wspólnych działaniach podjętych przez podmioty wchodzące w skład sektora bankowego i infrastruktury rynków finansowych, KNF, Ministra Finansów i odzwierciedlać założenia zawarte w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Wreszcie podkreślenia wymaga tzw. triada czynników umożliwiająca wprowadzenie efektywnej polityki cyberbezpieczeństwa. Należą do niej niewątpliwie dbałość o aktualność rozwiązań prawnych (strategia cyberbezpieczeństwa a powszechnie obowiązujące akty prawa) oraz kwestie (przystosowanie) technologiczne (oprogramowania, sprzęt, jakość sieci). Nie dziwi zatem wzrost zainteresowania nowymi technologiami na rynku finansowym. Spoiwem tych dwóch elementów są umiejętności (kompetencje) cyfrowe operatorów usług kluczowych, organów administracji publicznej, inwestorów, użytkowników indywidualnych.

W konkluzji należy przyznać, że współczesny wymiar bezpieczeństwa finansowego państwa to również wymiar bezpieczeństwa e-finansów. Kluczowym aspektem jest wdrożenie optymalnej polityki cyberbezpieczeństwa, ale również rozwój umiejętności (kompetencji) cyfrowych aktorów rynku finansowego.

Bibliografia

Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15 (8).

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Bartczak K., Bodych-Biernacka M., *Rodzaje cyberzagrożeń i prawne sposoby im przeciwdziałania w kontekście stosowania cyfrowych platform technologicznych w Polsce i UE*, „Przegląd Organizacji" 2021, nr 3 (974).

Błażewski M., *Środki komunikacji elektronicznej w prawie zamówień publicznych*, „Research Papers of Wrocław University of Economics" 2017, nr 497, DOI: 10.15611/pn.2017.497.19.

Chałubińska-Jentkiewicz K., *Bezpieczeństwo prawne danych osobowych w nowych warunkach cyfrowych*, „Zeszyty Naukowe Katolickiego Uniwersytetu Lubelskiego Jana Pawła II" 2018, nr 61 (1), DOI: 10.31743/zn.2018.61.1.179-196.

Drgas K., *Przesłanki wdrażania cyfryzacji jednostek samorządu lokalnego finansowanej ze środków unijnych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2019, nr 81 (1), DOI: 10.14746/rpeis.2019.81.1.13.

Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.

Klepacka P., Kowalewska E., *Instrumenty polityki pieniężnej w działalności Narodowego Banku Polskiego*, w: W. Bożek, E. Kowalewska (red.), *Bank i pieniądz w Polsce i na świecie*, Szczecin 2017.

Komisja Nadzoru Finansowego, *Departament Cyberbezpieczeństwa (DCB)*, www.knf.gov.pl/o_nas/urzad_komisji/dane_teleadresowe_struktura?articleId=65223&p_id=18.

Komisja Nadzoru Finansowego, *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego*, www.knf.gov.pl/dla_rynku/CSIRT_KNF.

Krawczyk-Jezierska A., *Koszty instytucji finansowych w świetle zagrożeń cybernetycznych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 8 (854).

Krzyżankiewicz F., *Ustawa o krajowym systemie cyberbezpieczeństwa. Identyfikacja i rejestracja operatorów usług kluczowych*, „Informacja w administracji publicznej" 2019, nr 1.

Monarcha-Matlak A., *Komunikacja elektroniczna, prawo komunikacji elektronicznej, Europejski kodeks łączności elektronicznej i ich wpływ na rozwój jurysdykcji administracyjnej*, w: M. Szewczyk, L. Staniszewska, M. Kruś (red.), *Kierunki rozwoju jurysdykcji administracyjnej*, Warszawa 2022.

Pisarewicz P., Kowalewska E., *Wybrane zagadnienia regulacji prawa bankowego i nadzoru nad rynkiem finansowym w kontekście praktyki ochrony klientów sektora bankowego*, „Zarządzanie i Finanse. Journal of Management and Finance" 2017, nr 2/1.

Pitera R., *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności" 2017, nr 2 (4).

Skoczylas D., *Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku*, w: M. Staniszewski, H.E. Kretek (red.), *Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonalenia warsztatu naukowca*, Gliwice 2021.

Skoczylas D., *Przetwarzanie danych osobowych a prawo do bycia zapomnianym i prawo do przenoszenia danych na gruncie RODO*, „Acta Iuris Stetinensis" 2018, nr 4 (24), DOI: 10.18276/ais.2018.24-04.

Skoczylas D., *The Act on the National Cybersecurity System and Other Legal Regulations in the Context of Ensuring State Cybersecurity. Selected Issues*, „Roczniki Nauk Prawnych" 2020, t. XXX, nr 2, DOI: 10.18290/rnp20302-7.

Szpor G., *Nowelizacja siatki pojęciowej cyberbezpieczeństwa*, „Monitor Prawniczy" 2020, nr 22.

Terlikowski T., *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)*, „Zeszyty Naukowe Szkoły Głównej Służby Pożarniczej" 2019, nr 71/3.

Widawski P., *Cyberbezpieczeństwo w usługach płatniczych*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Żywucka-Kozłowska E., Dziembowski R., *Społeczeństwo informacyjne w perspektywie wybranych aktów prawnych Unii Europejskiej*, „Media – Kultura – Komunikacja Społeczna" 2021, nr 3 (16), DOI: 10.31648/mkks.6620.

Cybersecurity of the Banking Sector and Financial Markets Infrastructure

Abstract

The article deals with the issue of cybersecurity in the banking sector and financial markets infrastructure. Considerations in this regard were carried out on the basis of an analysis of the provisions of the Act on the National Cybersecurity System. In addition, the current

principles of cybersecurity in the context of the tasks of the Financial Supervision Commission were taken into account. The paper uses the dogmatic-legal method.

The aim of the article is to characterise threats occurring in the banking sector and financial market infrastructure in connection with the provision of the so-called e-services in cyberspace. The subject of consideration is also the presentation and assessment of the current rules of cybersecurity and the tasks of the Financial Supervision Commission (competent authority for cybersecurity). A key aspect is also to indicate the activities undertaken by the right Computer Security Incident Response Team (CSIRT), especially in the context of classification and handling of network incidents. The analysis of the topic will answer the following question: what issues should be taken into account when implementing a cybersecurity policy in the banking sector and financial markets infrastructure.

The author of the paper has established that the contemporary dimension of the state financial security is also the dimension of e-financial security. Considering the above, the key aspect is the implementation of an optimal cybersecurity policy, but also the development of skills (competences) of digital actor of the financial market.

Keywords: cybersecurity, cyberthreats, Financial Supervision Commission, banking sector and financial market infrastructures, key services

CYTOWANIE

Skoczylas D., *Cyberbezpieczeństwo sektora bankowego i infrastruktury rynków finansowych*, „Acta Iuris Stetinensis" 2023, nr 2 (vol. 43), 107–122, DOI: 10.18276/ais.2023.43-06.