I

(Rezolucje, zalecenia i opinie)

ZALECENIA

EUROPEJSKA RADA DS. RYZYKA SYSTEMOWEGO

ZALECENIE EUROPEJSKIEJ RADY DS. RYZYKA SYSTEMOWEGO

z dnia 2 grudnia 2021 r.

w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym

(ERRS/2021/17)

(2022/C 134/01)

RADA GENERALNA EUROPEJSKIEJ RADY DS. RYZYKA SYSTEMOWEGO,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym ([1]), w szczególności załącznik IX,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1092/2010 z dnia 24 listopada 2010 r. w sprawie unijnego nadzoru makroostrożnościowego nad systemem finansowym i ustanowienia Europejskiej Rady ds. Ryzyka Systemowego ([2]), w szczególności art. 3 ust. 2 lit. b) i d) oraz art. 16 i art. 18,

uwzględniając decyzję Europejskiej Rady ds. Ryzyka Systemowego ERRS/2011/1 z dnia 20 stycznia 2011 r. ustanawiającą regulamin Europejskiej Rady ds. Ryzyka Systemowego ([3]), w szczególności art. 18–20,

a także mając na uwadze, co następuje:

(1) Zgodnie z motywem 4 rozporządzenia Europejskiej Rady ds. Ryzyka Systemowego ERRS/2013/1 ([4]) ostatecznym celem polityki makroostrożnościowej jest przyczynianie się do ochrony stabilności systemu finansowego jako całości, w tym poprzez wzmacnianie odporności systemu finansowego i ograniczanie powstawania ryzyk systemowych, a tym samym zapewnianie trwałego wkładu sektora finansowego do wzrostu gospodarczego. Europejska Rada ds. Ryzyka Systemowego (ERRS) jest odpowiedzialna za sprawowanie nadzoru makroostrożnościowego nad systemem finansowym w Unii. Wykonując swój mandat, ERRS powinna przyczyniać się do zapobiegania ryzyku systemowemu i do łagodzenia jego skutków, w tym związanych z cyberincydentami, a także proponować sposoby ograniczania tego ryzyka.

(2) Poważne cyberincydenty mogą stwarzać ryzyko systemowe dla systemu finansowego ze względu na możliwość zakłócenia przez nie kluczowych usług i operacji finansowych. Początkowy wstrząs może zostać spotęgowany przez efekt „zarażenia" operacyjnego lub finansowego albo w wyniku osłabienia zaufania do systemu finansowego. Jeżeli system finansowy nie będzie w stanie amortyzować tych wstrząsów, stabilność finansowa będzie zagrożona, a sytuacja ta może doprowadzić do kryzysu cybernetycznego o charakterze systemowym ([5]).

([1]) Dz.U. L 1 z 3.1.1994 r., s. 3.
([2]) Dz.U. L 331 z 15.12.2010, s. 1.
([3]) Dz.U. C 58 z 24.2.2011, s. 4.
([4]) Rozporządzenie Europejskiej Rady ds. Ryzyka Systemowego ERRS/2013/1 z dnia 4 kwietnia 2013 r. w sprawie celów pośrednich i instrumentów polityki makroostrożnościowej (Dz.U. C 170 z 15.6.2013, s. 1).
([5]) Zob. dokument pt. „Systemic cyber risk" [Systemowe ryzyko cybernetyczne], ERRS, luty 2020 r., dostępny na stronie internetowej ERRS pod adresem www.esrb.europa.eu

(3) Stale ewoluujący krajobraz zagrożeń cybernetycznych i niedawny wzrost liczby poważnych cyberincydentów wskazują na wyższe ryzyko dla stabilności finansowej w Unii. Pandemia COVID-19 uwydatniła rolę technologii w umożliwianiu funkcjonowania systemu finansowego. Odpowiednie organy i instytucje musiały dostosować swoją infrastrukturę techniczną i ramy zarządzania ryzykiem do nagłego wzrostu liczby osób pracujących zdalnie, co zwiększyło ogólne narażenie systemu finansowego na zagrożenia cybernetyczne i umożliwiło przestępcom zarówno opracowanie nowych sposobów działania, jak i dostosowanie istniejących metod w celu wykorzystania tej sytuacji ([6]). W tym kontekście liczba cyberincydentów zgłoszonych Nadzorowi Bankowemu EBC w 2020 r. wzrosła o 54 % w porównaniu z 2019 r ([7]).

(4) Potencjalnie duża skala, szybkość i tempo rozprzestrzeniania się poważnych cyberincydentów wymagają skutecznej reakcji ze strony odpowiednich organów w celu ograniczenia potencjalnych negatywnych skutków dla stabilności finansowej. Szybka koordynacja i komunikacja między odpowiednimi organami na poziomie Unii może ułatwić wczesną ocenę wpływu poważnego cyberincydentu na stabilność finansową, utrzymanie zaufania do systemu finansowego i ograniczenie efektu „zarażenia" innych instytucji finansowych, a tym samym przyczynić się do zapobieżenia sytuacji, w której poważny cyberincydent stałby się zagrożeniem dla stabilności finansowej.

(5) Wstrząs leżący u podstaw kryzysu ma nowatorski charakter w porównaniu z tradycyjnymi kryzysami finansowymi i płynnościowymi, z którymi dotychczas zmagały się odpowiednie organy. Oprócz aspektów finansowych ogólna ocena ryzyka musi obejmować skalę i skutki zakłóceń operacyjnych, ponieważ mogą one wpływać na wybór narzędzi makroostrożnościowych. Stabilność finansowa może również wpływać na wybór środków ograniczających ryzyko operacyjne przez specjalistów ds. cyberbezpieczeństwa. Wymaga to ścisłej i szybkiej koordynacji oraz otwartej komunikacji, m.in. w celu uzyskania orientacji sytuacyjnej.

(6) Zachodzi ryzyko niepowodzenia koordynacji po stronie organów, któremu należy przeciwdziałać. Konieczne będzie koordynowanie działań przez odpowiednie organy w Unii między sobą z innymi organami, takimi jak Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), z którymi zazwyczaj nie współdziałają. Ponieważ wiele unijnych instytucji finansowych działa na całym świecie, zachodzi duże prawdopodobieństwo, że poważny cyberincydent nie będzie ograniczony do obszaru Unii lub może zostać wywołany poza Unią i wymagać globalnej koordynacji działań.

(7) Odpowiednie organy muszą być przygotowane na takie interakcje. W przeciwnym razie zachodzi ryzyko podjęcia przez nie niespójnych działań, które będą sprzeczne z reakcjami innych organów lub będą im zagrażać. Taki brak koordynacji mógłby spotęgować wstrząs dla systemu finansowego, prowadząc do erozji zaufania do funkcjonowania systemu finansowego, co w najgorszym scenariuszu stanowiłoby zagrożenie dla stabilności finansowej ([8]). Należy zatem podjąć niezbędne kroki w celu przeciwdziałania zagrożeniu dla stabilności finansowej wynikającemu z niepowodzenia koordynacji w przypadku poważnego cyberincydentu.

(8) W sprawozdaniu ERRS z 2021 pt. „Mitigating systemic cyber risk" ([9]) wskazano na potrzebę ustanowienia paneuropejskich ram koordynacji dla odpowiednich organów w Unii w odniesieniu do cyberincydentów o charakterze systemowym (zwanych dalej „paneuropejskimi ramami koordynacji w odniesieniu do cyberincydentów systemowych"). Celem paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych byłoby zwiększenie poziomu gotowości odpowiednich organów w celu ułatwienia skoordynowanej reakcji na potencjalnie poważne cyberincydenty. We wspomnianym sprawozdaniu ERRS z 2021 r. przedstawiono dokonaną przez ERRS ocenę cech takich ram koordynacji, które, według wstępnych ustaleń, byłyby konieczne do ograniczenia ryzyka niepowodzenia koordynacji.

(9) Głównym celem niniejszego zalecenia jest wykorzystanie jednej z ról Europejskich Urzędów Nadzoru przewidzianych we wniosku dotyczącym rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego ([10]) (zwanego dalej „rozporządzeniem w sprawie operacyjnej odporności cyfrowej sektora finansowego") polegającej na stopniowym umożliwianiu skutecznej skoordynowanej reakcji na szczeblu Unii w przypadku poważnego transgranicznego incydentu związanego z technologiami teleinformatycznymi (ICT) lub powiązanego z takim incydentem zagrożenia mającego systemowy wpływ na cały sektor finansowy Unii. Proces ten doprowadzi do stworzenia paneuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów systemowych.

([6]) Zob. dokument pt. „Internet Organised Crime Threat Assessment" [Ocena zagrożenia przestępczością zorganizowaną w Internecie], Europol, 2020, dostępny na stronie internetowej Europolu pod adresem www.europol.europa.eu

([7]) Zob. dokument pt. „IT and cyber risk: a constant challenge" [Ryzyko informatyczne i cybernetyczne: ciągłe wyzwanie], EBC, 2021 r., dostępny na stronie internetowej Nadzoru Bankowego EBC pod adresem www.bankingsupervision.europa.eu

([8]) Zob. dokument pt. „Systemic cyber risk" [Systemowe ryzyko cybernetyczne], ERRS, luty 2020 r., dostępny na stronie internetowej ERRS pod adresem www.esrb.europa.eu

([9]) Zob. dokument pt. „Mitigating systemic cyber risk" [Ograniczanie systemowego ryzyka cybernetycznego], ERRS, 2021 r. (oczekuje na publikację).

([10]) COM/2020/595 final.

(10) Celem paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych nie powinno być zastąpienie istniejących ram, lecz wypełnienie ewentualnych luk w koordynacji i komunikacji między samymi odpowiednimi organami oraz między odpowiednimi organami a innymi organami w Unii oraz innymi kluczowymi podmiotami na poziomie międzynarodowym. W związku z tym należy rozważyć włączenie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych do istniejących ram dotyczących kryzysu finansowego i unijnych ram dotyczących cyberincydentów. Jeżeli chodzi o koordynację między odpowiednimi organami, należy wziąć pod uwagę między innymi role i działania grupy współpracy ds. bezpieczeństwa sieci i systemów informatycznych (NIS) dla podmiotów finansowych, o której mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 ([11]), mechanizmy koordynacji przewidziane w ramach utworzenia wspólnej jednostki ds. cyberprzestrzeni, a także zaangażowanie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa.

(11) W szczególności propozycja rozpoczęcia przygotowań do ustanowienia paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych ma na celu wyrażenie poparcia dla potencjalnych zadań Europejskich Urzędów Nadzoru, zgodnie z wnioskiem dotyczącym rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego. We wniosku tym stwierdza się, że: „Europejskie Urzędy Nadzoru, za pośrednictwem Wspólnego Komitetu i we współpracy z właściwymi organami, Europejskim Bankiem Centralnym (EBC) i ERRS, mogą ustanowić mechanizmy umożliwiające wymianę skutecznych praktyk między sektorami finansowymi, aby zwiększyć orientację sytuacyjną i zidentyfikować wspólne dla sektorów finansowych luki i rodzaje ryzyka w cyberprzestrzeni" oraz „mogą one opracować ćwiczenia z zakresu zarządzania kryzysowego i sytuacji awaryjnych obejmujące scenariusze cyberataków w celu wypracowania kanałów komunikacyjnych i stopniowego umożliwiania skutecznej skoordynowanej reakcji na poziomie UE w przypadku poważnego transgranicznego incydentu związanego z ICT lub powiązanego zagrożenia mającego systemowy wpływ na cały sektor finansowy Unii" ([12]). Nie istnieją jeszcze paneuropejskie ramy takie jak paneuropejskie ramy koordynacji w odniesieniu do cyberincydentów systemowych – należy je ustanowić i opracować w kontekście rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego.

(12) Biorąc pod uwagę zagrożenie dla stabilności finansowej w Unii wynikające z ryzyka cybernetycznego, prace przygotowawcze mające na celu stopniowe ustanowienie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych powinny, w miarę możliwości, rozpocząć się jeszcze przed pełnym wdrożeniem ram prawnych i politycznych wymaganych dla jego ustanowienia. Te ramy prawne i polityczne zostałyby w pełni ukończone i sfinalizowane po tym, jak zaczną obowiązywać odpowiednie przepisy rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego i aktów delegowanych na podstawie tego rozporządzenia.

(13) Skuteczna komunikacja przyczynia się do poprawy orientacji sytuacyjnej wśród odpowiednich organów, a zatem stanowi niezbędny warunek wstępny ogólnounijnej koordynacji podczas poważnych cyberincydentów. W związku z tym należy zdefiniować infrastrukturę komunikacyjną niezbędną do koordynowania reakcji na poważny cyberincydent. Oznaczałoby to określenie rodzaju informacji, które powinny być udostępniane, regularnych kanałów wymiany takich informacji oraz punktów kontaktowych, którym informacje powinny być przekazywane. Wymiana informacji musi być zgodna z obowiązującymi wymogami prawnymi. Ponadto konieczne może być opracowanie przez odpowiednie organy jasnego planu działania i protokołów, których należy przestrzegać, aby zapewnić właściwą koordynację między organami zaangażowanymi w planowanie skoordynowanej reakcji na poważny cyberincydent.

(14) Kryzys cybernetyczny o charakterze systemowym będzie wymagał pełnej współpracy na szczeblu krajowym i unijnym. W związku z tym można zaplanować wyznaczenie punktów kontaktowych dla Europejskich Urzędów Nadzoru, EBC i dla każdego państwa członkowskiego spośród ich odpowiednich organów krajowych w celu ustanowienia głównych podmiotów w paneuropejskich ramach koordynacji w odniesieniu do cyberincydentów systemowych, które będą informowane w przypadku wystąpienia poważnego cyberincydentu. Podczas opracowywania paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych należy ocenić potrzebę wyznaczenia punktów kontaktowych, biorąc pod uwagę pojedynczy punkt kontaktowy przewidziany dyrektywą (UE) 2016/1148, który państwa członkowskie ustanowiły w zakresie bezpieczeństwa sieci i systemów informatycznych w celu zapewnienia współpracy transgranicznej z innymi państwami członkowskimi oraz z Grupą Współpracy ds. bezpieczeństwa sieci i systemów informatycznych ([13]).

(15) Prowadzenie ćwiczeń w zakresie zarządzania kryzysowego i sytuacji awaryjnych mogłoby ułatwić wdrożenie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych oraz umożliwić organom ocenę ich gotowości i stanu przygotowania na kryzys cybernetyczny o charakterze systemowym na poziomie Unii. Takie ćwiczenia pozwoliłyby organom na zdobycie doświadczenia oraz umożliwiłyby ciągłe usprawnianie i doskonalenie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych.

([11]) Dyrektywa 2016/1148 Parlamentu Europejskiego i Rady z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194, 19.7.2016, s. 1).

([12]) Zob. proponowany art. 43 wniosku dotyczącego rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego.

([13]) Zob. Komisja Europejska, Grupa Współpracy ds. bezpieczeństwa sieci i systemów informatycznych, dostępna na stronie internetowej Komisji Europejskiej pod adresem www.ec.europa.eu

(16) Aby opracować paneuropejskie ramy koordynacji w odniesieniu do cyberincydentów systemowych, konieczne jest wspólne przeprowadzenie przez Europejskie Urzędy Nadzoru odpowiednich prac przygotowawczych w celu określenia potencjalnych kluczowych elementów tych ram, niezbędnych zasobów oraz potrzeb związanych z ich opracowaniem. Następnie Europejskie Urzędy Nadzoru mogłyby rozpocząć prace nad wstępną analizą ewentualnych przeszkód, które mogłyby utrudnić Europejskim Urzędom Nadzoru i odpowiednim organom ustanowienie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych i wymianę istotnych informacji za pośrednictwem kanałów komunikacyjnych w przypadku poważnego cyberincydentu. Taka analiza stanowiłaby ważny krok poprzedzający wszelkie dalsze działania, zarówno o charakterze legislacyjnym, jak i inne inicjatywy wspierające, które Komisja Europejska może podjąć na etapie implementacji po przyjęciu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego,

PRZYJMUJE NINIEJSZE ZALECENIE:

SEKCJA 1

ZALECENIA

Zalecenie A – Ustanowienie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów o charakterze systemowym

1. Zaleca się, aby – zgodnie z założeniami wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (zwanego dalej „rozporządzeniem w sprawie operacyjnej odporności cyfrowej sektora finansowego") – Europejskie Urzędy Nadzoru (ESA), wspólnie, za pośrednictwem Wspólnego Komitetu, i wraz z Europejskim Bankiem Centralnym (EBC), Europejską Radą ds. Ryzyka Systemowego (ERRS) i odpowiednimi organami krajowymi rozpoczęły przygotowania do stopniowego opracowywania skutecznej skoordynowanej reakcji na poziomie Unii na wypadek poważnych transgranicznych cyberincydentów lub związanych z nimi zagrożeń, które mogą mieć systemowy wpływ na unijny sektor finansowy. Prace przygotowawcze do skoordynowanej reakcji na poziomie Unii powinny obejmować stopniowe opracowanie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych dla Europejskich Urzędów Nadzoru, EBC, ERRS i odpowiednich organów krajowych. Prace te powinny również obejmować ocenę zapotrzebowania na zasoby konieczne do skutecznego opracowania tych ram.

2. Zaleca się, aby w świetle zalecenia A(1) Europejskie Urzędy Nadzoru, w porozumieniu z EBC i ERRS, podjęły się mapowania oraz późniejszej analizy obecnych przeszkód, barier prawnych i innych barier operacyjnych dla skutecznego opracowania paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych.

Zalecenie B – Ustanowienie punktów kontaktowych dla paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych

Zaleca się, aby Europejskie Urzędy Nadzoru, EBC i każde z państw członkowskich (spośród swoich odpowiednich organów krajowych) wyznaczyły swój główny punkt kontaktowy, o którym powinny zostać poinformowane Europejskie Urzędy Nadzoru. Ta lista punktów kontaktowych ułatwi opracowanie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych, a po ich wprowadzeniu punkty kontaktowe i ERRS powinny być informowane w przypadku wystąpienia poważnego cyberincydentu. Należy również przewidzieć koordynację między paneuropejskimi ramami koordynacji w odniesieniu do cyberincydentów systemowych a wyznaczonym pojedynczym punktem kontaktowym, o którym mowa w dyrektywie (UE) 2016/1148, który państwa członkowskie ustanowiły w zakresie bezpieczeństwa sieci i systemów informatycznych w celu zapewnienia współpracy transgranicznej z innymi państwami członkowskimi oraz z Grupą Współpracy ds. bezpieczeństwa sieci i systemów informatycznych.

Zalecenie C – Odpowiednie środki na poziomie Unii

Zaleca się, aby w oparciu o wyniki analiz przeprowadzonych zgodnie z zaleceniem A Komisja rozważyła odpowiednie środki niezbędne do zapewnienia skutecznej koordynacji reakcji na cyberincydenty systemowe.

SEKCJA 2

IMPLEMENTACJA

1. **Definicje**

Użyte w niniejszym zaleceniu wyrażenia oznaczają:

a) „cyber-" lub „cybernetyczny" – związany ze wzajemnie połączoną infrastrukturą informatyczną, w ramach której zachodzą interakcje między osobami, procesami, danymi i systemami informatycznymi, istniejący w ramach tej infrastruktury lub zachodzący za jej pośrednictwem ([14]);

([14]) Zob. publikacja „Cyber Lexicon", Rada Stabilności Finansowej, 12 listopada 2018 r., dostępna na stronie internetowej Rady Stabilności Finansowej pod adresem www.fsb.org

b) „poważny cyberincydent" – incydent związany z technologiami teleinformatycznymi o potencjalnie dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne funkcje podmiotów finansowych ([15]);

c) „kryzys cybernetyczny o charakterze systemowym" – poważny cyberincydent, który powoduje poziom zakłóceń w systemie finansowym Unii potencjalnie pociągający za sobą poważne negatywne skutki dla sprawnego funkcjonowania rynku wewnętrznego i funkcjonowania gospodarki realnej. Taki kryzys może wynikać z poważnego cyberincydentu powodującego wstrząsy w wielu wymiarach, w tym w wymiarze operacyjnym, związanym z zaufanym oraz finansowym;

d) „Europejskie Urzędy Nadzoru" – europejski organ nadzoru (Europejski Organ Nadzoru Bankowego) ustanowiony na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([16]) wraz z europejskim organem nadzoru (Europejskim Urzędem Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych) ustanowionym na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 1094/2010 ([17]) oraz europejskim organem nadzoru (Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych) ustanowionym na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([18]);

e) „Wspólny Komitet" – Wspólny Komitet Europejskich Urzędów Nadzoru ustanowiony na mocy art. 54 rozporządzenia (UE) nr 1093/2010, art. 54 rozporządzenia (UE) nr 1094/2010, i w art. 54 rozporządzenia (UE) nr 1095/2010;

f) „odpowiedni organ krajowy" –

1. właściwy organ lub organ nadzorczy państwa członkowskiego określony w prawnie wiążących aktach Unii, o których mowa w art. 1 ust. 2 rozporządzenia (UE) nr 1093/2010, art. 1 ust. 2 rozporządzenia (UE) nr 1094/2010 oraz art. 1 ust. 2 rozporządzenia (UE) nr 1095/2010, oraz każdy inny właściwy organ krajowy określony w aktach Unii powierzających zadania Europejskim Urzędom Nadzoru;

2. właściwy organ w państwie członkowskim wyznaczony zgodnie z:

i. art. 4 dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE ([19]), bez uszczerbku dla szczególnych zadań powierzonych EBC na mocy rozporządzenia Rady (UE) nr 1024/2013 ([20]);

ii. art. 22 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 ([21]);

iii. art. 37 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE ([22]);

iv. art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/2034 ([23]);

([15]) Zob. art. 3 pkt 7 wniosku dotyczącego rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego.

([16]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

([17]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.U. L 331 z 15.12.2010, s. 48).

([18]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1095/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/77/WE (Dz.U. L 331 z 15.12.2010, s. 84).

([19]) Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

([20]) Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz.U. L 287 z 29.10.2013, s. 63).

([21]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

([22]) Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz.U. L 267 z 10.10.2009, s. 7).

([23]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2034 z dnia 27 listopada 2019 r. w sprawie nadzoru ostrożnościowego nad firmami inwestycyjnymi oraz zmieniająca dyrektywy 2002/87/WE, 2009/65/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE i 2014/65/UE (Dz.U. L z 314 z 5 grudnia 2019, s. 64).

v. art. 3 ust. 1 lit. ee) tiret pierwsze wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937 ([24]);

vi. art. 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 909/2014 ([25]);

vii. art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 ([26]);

viii. art. 67 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE ([27]):

ix. art. 22 rozporządzenia (UE) nr 648/2012;

x. art. 44 dyrektywy Parlamentu Europejskiego i Rady 2011/61/UE ([28]);

xi. art. 97 dyrektywy Parlamentu Europejskiego i Rady 2009/65/WE ([29]);

xii. art. 30 dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE ([30]);

xiii. art. 12 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/97 ([31]);

xiv. art. 47 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2341 ([32]);

xv. art. 22 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1060/2009 ([33]);

xvi. art. 3 ust. 2 i art. 32 dyrektywy Parlamentu Europejskiego i Rady 2006/43/WE ([34]);

xvii. art. 40 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/1011 ([35]);

xviii. art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2020/1503 ([36]);

([24]) COM/2020/593 final.

([25]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U. L 257 z 28.8.2014, s. 1).

([26]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 201 z 27.7.2012, s. 1).

([27]) Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).

([28]) Dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010 (Dz.U. L 174 z 1.7.2011, s. 1).

([29]) Dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS) (Dz.U. L 302 z 17.11.2009, s. 32).

([30]) Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 335 z 17.12.2009, s. 1).

([31]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń (wersja przekształcona) (Dz.U. L 26 z 2.2.2016, s. 19).

([32]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2341 z dnia 14 grudnia 2016 r. w sprawie działalności instytucji pracowniczych programów emerytalnych oraz nadzoru nad takimi instytucjami (IORP) (Dz.U. L 354 z 23.12.2016, s. 37).

([33]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1060/2009 z dnia 16 września 2009 r. w sprawie agencji ratingowych (Dz.U. L 302 z 17.11.2009, s. 1).

([34]) Dyrektywa Parlamentu Europejskiego i Rady 2006/43/WE z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, zmieniająca dyrektywy Rady 78/660/EWG i 83/349/EWG oraz uchylająca dyrektywę Rady 84/253/EWG (Dz.U. L 157 z 9.6.2006, s. 87).

([35]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1011 z dnia 8 czerwca 2016 r. w sprawie indeksów stosowanych jako wskaźniki referencyjne w instrumentach finansowych i umowach finansowych lub do pomiaru wyników funduszy inwestycyjnych i zmieniające dyrektywy 2008/48/WE i 2014/17/UE oraz rozporządzenie (UE) nr 596/2014 (Dz.U. L 171 z 29.6.2016, s. 1).

([36]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/1503 z dnia 7 października 2020 r. w sprawie europejskich dostawców usług finansowania społecznościowego dla przedsięwzięć gospodarczych oraz zmieniające rozporządzenie (UE) 2017/1129 i dyrektywę (UE) 2019/1937 (Dz.U. L 347 z 20.10.2020, s. 1).

3. organ, któremu powierzono przyjęcie lub uruchomienie środków polityki makroostrożnościowej lub inne zadania w zakresie stabilności finansowej, takie jak odpowiednia analiza uzupełniająca, w tym między innymi:

   i. wyznaczony organ na podstawie rozdziału 4 tytułu VII dyrektywy 2013/36/UE lub art. 458 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 ([37]);

   ii. organ makroostrożnościowy o celach, ustaleniach, zadaniach, uprawnieniach, instrumentach i wymogach w zakresie odpowiedzialności i innych cechach wskazanych w zaleceniu Europejskiej Rady ds. Ryzyka Systemowego ERRS/2011/3 ([38]);

g) „odpowiedni organ" –

   1. Europejski Urząd Nadzoru;

   2. EBC w zakresie zadań powierzonych mu zgodnie z art. 4 ust. 1 i 2 oraz art. 5 ust. 2 rozporządzenia (UE) nr 1024/2013;

   3. odpowiedni organ krajowy.

2. **Kryteria implementacji**

Do implementacji niniejszego zalecenia stosuje się następujące kryteria:

a) powinny zostać zachowane zasada wiedzy koniecznej i zasada proporcjonalności, przy uwzględnieniu celu i treści każdego z zaleceń;

b) powinny zostać spełnione szczególne kryteria zgodności określone w załączniku w odniesieniu do każdego zalecenia.

3. **Harmonogram informowania o realizacji zaleceń**

Zgodnie z art. 17 ust. 1 rozporządzenia (UE) nr 1092/2010 adresaci są zobowiązani poinformować Parlament Europejski, Radę, Komisję i ERRS o działaniach podjętych w odpowiedzi na niniejsze zalecenie lub przedstawić odpowiednie uzasadnienie w przypadku braku działania. Adresaci przekazują takie informacje w następujących terminach:

1. Zalecenie A

   a) Do dnia 30 czerwca 2023 r., jednak nie wcześniej niż po upływie sześciu miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, Europejskie Urzędy Nadzoru są zobowiązane przedstawić Parlamentowi Europejskiemu, Radzie, Komisji i ERRS sprawozdanie okresowe z realizacji zalecenia A(1).

   b) Do dnia 30 czerwca 2024 r., jednak nie wcześniej niż po upływie 18 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, Europejskie Urzędy Nadzoru są zobowiązane przedstawić Parlamentowi Europejskiemu, Radzie, Komisji i ERRS sprawozdanie końcowe z realizacji zalecenia A(1).

   c) Do dnia 30 czerwca 2025 r., jednak nie wcześniej niż po upływie 30 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, Europejskie Urzędy Nadzoru są zobowiązane przedstawić Parlamentowi Europejskiemu, Radzie, Komisji i ERRS sprawozdanie z realizacji zalecenia A(2).

2. Zalecenie B

   Do dnia 30 czerwca 2023 r., jednak nie wcześniej niż po upływie sześciu miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, Europejskie Urzędy Nadzoru, EBC i państwa członkowskie są zobowiązane przedstawić Parlamentowi Europejskiemu, Radzie, Komisji i ERRS sprawozdanie z realizacji zalecenia B.

3. Zalecenie C

   a) Do dnia 31 grudnia 2023 r., jednak nie wcześniej niż po upływie 12 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, Komisja jest zobowiązana przedstawić Parlamentowi Europejskiemu, Radzie i ERRS sprawozdanie z realizacji zalecenia C w świetle sprawozdania okresowego Europejskich Urzędów Nadzoru zgodnie z zaleceniem A(1).

([37]) Rozporządzenie Parlamentu Europejskiego i rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1)

([38]) Zalecenie Europejskiej Rady ds. Ryzyka Systemowego ERRS/2011/3 z dnia 22 grudnia 2011 r. w sprawie mandatu makroostrożnościowego organów krajowych (Dz.U. C 41 z 14.2.2012, s. 1).

b) Do dnia 31 grudnia 2025 r., jednak nie wcześniej niż po upływie 36 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, Komisja jest zobowiązana przedstawić Parlamentowi Europejskiemu, Radzie i ERRS sprawozdanie z realizacji zalecenia C w świetle sprawozdań Europejskich Urzędów Nadzoru zgodnie z zaleceniem A.

4. **Monitorowanie i ocena**

1. Sekretariat ERRS:

a) udziela pomocy adresatom poprzez zapewnianie koordynacji składania sprawozdań i dostarczanie odpowiednich wzorów i formularzy oraz, w razie potrzeby, szczegółowe określanie procedury i terminów informowania o realizacji zaleceń;

b) weryfikuje realizację zaleceń przez adresatów, udziela im pomocy na ich wniosek oraz przedkłada Radzie Generalnej sprawozdania dotyczące realizacji zaleceń. Przeprowadzone zostaną oceny, która rozpoczną się w następujących terminach:

(i) w terminie 12 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego – w odniesieniu do realizacji zaleceń A i B;

(ii) w terminie 18 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego – w odniesieniu do realizacji zalecenia C;

(iii) w terminie 24 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego – w odniesieniu do realizacji zalecenia A;

(iv) w terminie 36 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego – w odniesieniu do realizacji zalecenia A;

(v) w terminie 42 miesięcy od wejścia w życie rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego – w odniesieniu do realizacji zalecenia C.

2. Rada Generalna ocenia działania adresatów i przedstawiane przez nich uzasadnienia oraz, w razie potrzeby, może stwierdzić nieodpowiednie zastosowanie się do niniejszego zalecenia lub brak odpowiedniego uzasadnienia niepodjęcia działań.

Sporządzono we Frankfurcie nad Menem dnia 2 grudnia 2021 r.

W imieniu Rady Generalnej ERRS
Francesco MAZZAFERRO
Szef Sekretariatu ERRS

ZAŁĄCZNIK

OKREŚLENIE KRYTERIÓW ZGODNOŚCI W ODNIESIENIU DO ZALECEŃ

Zalecenie A – Ustanowienie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów o charakterze systemowym

W odniesieniu do zalecenia A(1) określa się następujące kryteria zgodności.

1. Przygotowując się do skutecznej skoordynowanej reakcji na szczeblu Unii, która powinna obejmować stopniowe opracowanie paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych poprzez wykonywanie uprawnień przewidzianych w planowanym rozporządzeniu Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (zwanego dalej „rozporządzeniem w sprawie operacyjnej odporności cyfrowej sektora finansowego"), Europejskie Urzędy Nadzoru (ESA), działające za pośrednictwem Wspólnego Komitetu i wraz z Europejskim Bankiem Centralnym (EBC), Europejską Radą ds. Ryzyka Systemowego (ERRS) i odpowiednimi organami krajowymi, a także w porozumieniu z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji oraz Komisją, jeżeli zostanie to uznane za konieczne, powinny rozważyć uwzględnienie w planowanych przygotowaniach do paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych co najmniej takich aspektów jak:

   a. analiza zapotrzebowania na zasoby konieczne do skutecznego opracowania paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych;

   b. opracowywanie ćwiczeń w zakresie zarządzania kryzysowego i sytuacji awaryjnych obejmujących scenariusze cyberataków w celu wypracowania kanałów komunikacyjnych;

   c. opracowanie wspólnej nomenklatury;

   d. opracowanie spójnej klasyfikacji cyberincydentów;

   e. ustanowienie bezpiecznych i niezawodnych kanałów wymiany informacji, w tym systemów kopii zapasowych;

   f. ustanowienie punktów kontaktowych;

   g. uwzględnienie poufności w procesie wymiany informacji;

   h. inicjatywy w zakresie współpracy i wymiany informacji z wywiadem cybernetycznym sektora finansowego;

   i. opracowanie skutecznych procedur aktywizacji i eskalacji poprzez orientację sytuacyjną;

   j. sprecyzowanie zakresu odpowiedzialności uczestników ram;

   k. opracowanie interfejsów na potrzeby koordynacji międzysektorowej oraz, w stosownych wypadkach, koordynacji w odniesieniu do państw trzecich;

   l. zapewnienie spójnej komunikacji odpowiednich organów ze społeczeństwem w celu utrzymania zaufania;

   m. ustanowienie z góry określonych linii komunikacyjnych na potrzeby terminowej komunikacji;

   n. przeprowadzanie odpowiednich testów ram, w tym testów obejmujących różne jurysdykcje i koordynację z krajami trzecimi, oraz ocen skutkujących wyciągnięciem wniosków i ewolucją ram;

   o. zapewnienie skutecznej komunikacji i środków przeciwdziałania dezinformacji.

Zalecenie B – Ustanowienie punktów kontaktowych dla paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych

W odniesieniu do zalecenia B określa się następujące kryteria zgodności.

1. Europejskie Urzędy Nadzoru, EBC i każde państwo członkowskie w ramach swoich odpowiednich organów krajowych powinny uzgodnić wspólne podejście do udostępniania i aktualizowania wyznaczonych punktów kontaktowych paneuropejskich ram koordynacji w odniesieniu do cyberincydentów systemowych.

2. Wyznaczenie punktu kontaktowego powinno być ocenione przy uwzględnieniu wyznaczonego pojedynczego punktu kontaktowego, o którym mowa w dyrektywie (UE) 2016/1148, który państwa członkowskie ustanowiły w zakresie bezpieczeństwa sieci i systemów informatycznych w celu zapewnienia współpracy transgranicznej z innymi państwami członkowskimi oraz z Grupą Współpracy ds. bezpieczeństwa sieci i systemów informatycznych.

Zalecenie C – Zmiany w unijnych ramach prawnych

W odniesieniu do zalecenia C określa się następujące kryteria zgodności.

Komisja powinna rozważyć, czy w wyniku analizy przeprowadzonej zgodnie z zaleceniem A potrzebne są środki, w tym zmiany w odpowiednim prawodawstwie Unii, w celu zapewnienia Europejskim Urzędom Nadzoru – za pośrednictwem Wspólnego Komitetu oraz wspólnie z EBC, ERRS i odpowiednimi organami krajowymi – możliwości opracowania paneuropejskich ram koordynacji w odniesieniu do cyberincydentów o charakterze systemowym zgodnie z zaleceniem A(1) oraz w celu zapewnienia Europejskim Urzędom Nadzoru, EBC, ERRS i odpowiednim organom krajowym oraz innym organom możliwości angażowania się w działania koordynacyjne i wymianę informacji, które są wystarczająco szczegółowe i spójne, aby wspierać skuteczne ramy koordynacji w odniesieniu do cyberincydentów o charakterze systemowym.