Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/1772

25.6.2024

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2024/1772

z dnia 13 marca 2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 ([1]), w szczególności jego art. 18 ust. 4 akapit trzeci,

a także mając na uwadze, co następuje:

(1) Rozporządzenie (UE) 2022/2554 ma na celu harmonizację i uproszczenie wymogów w zakresie zgłaszania incydentów związanych z ICT oraz incydentów operacyjnych lub incydentów w zakresie bezpieczeństwa związanych z płatnościami dotyczących instytucji kredytowych, instytucji płatniczych, dostawców świadczących usługę dostępu do informacji o rachunku i instytucji pieniądza elektronicznego („incydenty"). Biorąc pod uwagę, że wymogi dotyczące zgłaszania obejmują 20 różnych rodzajów podmiotów finansowych, kryteria klasyfikacji i progi istotności do celów ustalania poważnych incydentów i znaczących cyberzagrożeń należy określić w prosty, zharmonizowany i spójny sposób, uwzględniający specyfikę usług i działań wykonywanych przez wszystkie odpowiednie podmioty finansowe.

(2) Aby zapewnić proporcjonalność, kryteria klasyfikacji i progi istotności powinny odzwierciedlać wielkość i ogólny profil ryzyka oraz charakter, skalę i złożoność usług świadczonych przez wszystkie podmioty finansowe. Ponadto kryteria i progi istotności należy opracować w taki sposób, aby miały one spójne zastosowanie do wszystkich podmiotów finansowych, niezależnie od ich wielkości i profilu ryzyka, oraz aby nie stanowiły nieproporcjonalnego obciążenia sprawozdawczego dla mniejszych podmiotów finansowych. Aby jednak uwzględnić sytuacje, w których incydent, który jako taki nie przekracza mającego zastosowanie progu, dotyczy znacznej liczby klientów, należy określić bezwzględny próg skierowany głównie do większych podmiotów finansowych.

(3) W odniesieniu do ram zgłaszania incydentów, które istniały przed wejściem w życie rozporządzenia (UE) 2022/2554, należy zapewnić podmiotom finansowym ciągłość. W związku z tym kryteria klasyfikacji i progi istotności powinny zostać opracowane na podstawie i dostosowane do wytycznych EUNB w sprawie zgłaszania poważnych incydentów na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 ([2]), wytycznych w sprawie okresowych informacji i powiadamiania o istotnych zmianach, które mają być przekazywane ESMA przez repozytoria transakcji, ram EBC/SSM dotyczących zgłaszania cyberincydentów oraz innych odpowiednich wytycznych. Kryteria klasyfikacji i progi powinny być również odpowiednie dla podmiotów finansowych, które nie podlegały wymogom dotyczącym zgłaszania incydentów przed wejściem w życie rozporządzenia (UE) 2022/2554.

(4) W odniesieniu do kryterium klasyfikacji „kwota lub liczba transakcji, których dotyczy incydent", pojęcie transakcji jest szerokie i obejmuje różne rodzaje działania i usługi uwzględnione w różnych aktach sektorowych mających zastosowanie do podmiotów finansowych. Do celów tego kryterium klasyfikacji należy uwzględnić transakcje płatnicze i wszelkie formy wymiany instrumentów finansowych, kryptoaktywów, towarów lub wszelkich innych aktywów, również w formie depozytu zabezpieczającego, zabezpieczenia lub zastawu, zarówno w zamian za środki pieniężne, jak i za wszelkie inne aktywa. Do celów klasyfikacji należy uwzględnić wszystkie transakcje dotyczące aktywów, których wartość może być wyrażona w kwocie pieniężnej.

([1]) Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj

([2]) 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, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Kryteria klasyfikacji powinny zapewniać uwzględnienie wszystkich istotnych rodzajów poważnych incydentów. Cyberataki związane z włamaniem do sieci lub systemów informatycznych niekoniecznie muszą być objęte wieloma kryteriami klasyfikacji. Są one jednak ważne, ponieważ wszelkie włamania do sieci i systemów informatycznych mogą zaszkodzić podmiotowi finansowemu. W związku z tym kryteria klasyfikacji „Usługi krytyczne, których dotyczy incydent", i „Utrata danych" należy określić w taki sposób, aby uchwycić te rodzaje poważnych incydentów, w szczególności włamania, które – nawet jeżeli ich skutki nie są natychmiast znane – mogą prowadzić do poważnych konsekwencji, w szczególności naruszeń ochrony danych i wycieków danych.

(6) Ponieważ instytucje kredytowe podlegają zarówno ramom klasyfikacji incydentów na podstawie art. 18 rozporządzenia (UE) 2022/2554, jak i ramom ryzyka operacyjnego na podstawie rozporządzenia delegowanego Komisji (UE) 2018/959 ([3]), podejście do oceny skutków gospodarczych incydentu w oparciu o obliczenie kosztów i strat powinno być w jak największym stopniu spójne w obu tych ramach, aby uniknąć wprowadzania niekompatybilnych lub sprzecznych wymogów.

(7) Kryterium dotyczące zasięgu geograficznego incydentu określone w art. 18 ust. 1 lit. c) rozporządzenia (UE) 2022/2554 powinno koncentrować się na transgranicznych skutkach incydentu, ponieważ wpływ incydentu na działania podmiotu finansowego w ramach jednej jurysdykcji zostanie uwzględniony w ramach pozostałych kryteriów określonych w tym artykule.

(8) Biorąc pod uwagę, że kryteria klasyfikacji są współzależne i wzajemnie ze sobą powiązane, podejście do identyfikacji poważnych incydentów, które należy zgłaszać zgodnie z art. 19 ust. 1 rozporządzenia (UE) 2022/2554, powinno opierać się na połączeniu kryteriów, przy czym niektóre kryteria ściśle powiązane z definicjami incydentu związanego z ICT i poważnego incydentu związanego z ICT określonymi w art. 3 pkt 8 i 10 rozporządzenia (UE) 2022/2554 powinny mieć większe znaczenie w klasyfikacji poważnych incydentów niż inne kryteria.

(9) W celu zapewnienia, aby zgłoszenia i powiadomienia dotyczące poważnych incydentów otrzymywane przez właściwe organy na podstawie art. 19 ust. 1 rozporządzenia (UE) 2022/2554 służyły zarówno do celów nadzorczych, jak i do zapobiegania zarażaniu w całym sektorze finansowym, progi istotności powinny umożliwiać uwzględnienie poważnych incydentów, koncentrując się m.in. na wpływie na usługi krytyczne specyficzne dla danego podmiotu, na konkretnych bezwzględnych i względnych progach klientów lub kontrahentów finansowych, transakcjach, które wskazują na istotny wpływ na podmiot finansowy, oraz na znaczeniu skutków incydentu w innych państwach członkowskich.

(10) Incydenty, które mają wpływ na usługi ICT lub sieci i systemy informatyczne wspierające krytyczne lub istotne funkcje lub na usługi finansowe wymagające upoważnienia, lub złośliwy nieuprawniony dostęp do sieci i systemów informatycznych, które wspierają krytyczne lub istotne funkcje, należy uznać za incydenty mające wpływ na usługi o krytycznym znaczeniu świadczone przez podmioty finansowe. Złośliwy, nieuprawniony dostęp do sieci i systemów informatycznych, które wspierają krytyczne lub istotne funkcje podmiotów finansowych, stwarza poważne ryzyko dla podmiotu finansowego i – ponieważ może mieć wpływ na inne podmioty finansowe – należy go zawsze uznawać za poważny incydent podlegający zgłoszeniu.

(11) Powtarzające się incydenty powiązane ze sobą podobną widoczną podstawową przyczyną, które pojedynczo nie są poważnymi incydentami, mogą wskazywać na znaczące niedoskonałości i słabości procedur zarządzania incydentami i ryzykiem stosowanych przez podmiot finansowy. W związku z tym powtarzające się incydenty należy uznać za poważne łącznie, jeżeli występują one wielokrotnie w określonym czasie.

(12) Biorąc pod uwagę, że cyberzagrożenia mogą mieć negatywne skutki dla podmiotu finansowego i sektora finansowego, opis znaczących cyberzagrożeń, które podmioty finansowe mogą zgłaszać, powinien wskazywać prawdopodobieństwo ich urzeczywistnienia i krytyczność potencjalnych skutków. W związku z tym, aby zapewnić jasną i spójną ocenę znaczenia cyberzagrożeń, klasyfikacja cyberzagrożenia jako znaczącego powinna zależeć od prawdopodobieństwa, czy w przypadku urzeczywistnienia się cyberzagrożenia kryteria klasyfikacji poważnych incydentów zostałyby spełnione, a ich próg został osiągnięty, od rodzaju cyberzagrożenia oraz od informacji, do których ma dostęp podmiot finansowy.

([3]) Rozporządzenie delegowane Komisji (UE) 2018/959 z dnia 14 marca 2018 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 w odniesieniu do regulacyjnych standardów technicznych określających metodę oceny, w ramach której właściwe organy zezwalają instytucjom na stosowanie metod zaawansowanego pomiaru na potrzeby obliczania ryzyka operacyjnego (Dz.U. L 169 z 6.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Biorąc pod uwagę obowiązek powiadamiania właściwych organów w innych państwach członkowskich o wystąpieniu incydentów, które mają wpływ na podmioty finansowe i klientów w ich jurysdykcji, ocena skutków w innej jurysdykcji zgodnie z art. 19 ust. 7 rozporządzenia (UE) 2022/2554 powinna opierać się na podstawowej przyczynie incydentu, na potencjalnym zarażeniu za pośrednictwem dostawców będących osobami trzecimi i infrastruktury rynku finansowego, a także na wpływie incydentu na znaczące grupy klientów lub kontrahentów finansowych.

(14) Procesy zgłaszania i powiadamiania, o których mowa w art. 19 ust. 6 i 7 rozporządzenia (UE) 2022/2554, powinny umożliwiać odpowiednim odbiorcom ocenę skutków incydentów. W związku z tym przekazywane informacje powinny obejmować wszystkie szczegóły zawarte w zgłoszeniach incydentów przedkładanych właściwemu organowi przez podmiot finansowy.

(15) Jeżeli incydent stanowi naruszenie ochrony danych osobowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) i dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady ([5]), niniejsze rozporządzenie nie powinno mieć wpływu na określone w tych aktach Unii obowiązki w zakresie rejestrowania naruszeń ochrony danych osobowych i powiadamiania o nich. Właściwe organy powinny współpracować ze sobą oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii z organami, o których mowa w rozporządzeniu (UE) 2016/679 i dyrektywie 2002/58/WE.

(16) Podstawę niniejszego rozporządzenia stanowią projekty regulacyjnych standardów technicznych przedłożone Komisji przez Europejskie Urzędy Nadzoru, po konsultacji z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz Europejskim Bankiem Centralnym (EBC).

(17) Wspólny Komitet Europejskich Urzędów Nadzoru, o którym mowa w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([6]), w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1094/2010 ([7]) i w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([8]), przeprowadził otwarte konsultacje publiczne na temat projektu regulacyjnych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, dokonał analizy potencjalnych powiązanych kosztów i korzyści oraz zwrócił się o opinię do Bankowej Grupy Interesariuszy powołanej zgodnie z art. 37 rozporządzenia (UE) nr 1093/2010, do Grupy Interesariuszy z Sektora Ubezpieczeń i Reasekuracji i Grupy Interesariuszy z Sektora Pracowniczych Programów Emerytalnych powołanych zgodnie z art. 37 rozporządzenia (UE) nr 1094/2010 oraz do Grupy Interesariuszy z Sektora Giełd i Papierów Wartościowych powołanej zgodnie z art. 37 rozporządzenia (UE) nr 1095/2010.

([4]) 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.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony (Dz.U. L 201 z 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([9]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który swoją opinię wydał 24 stycznia 2024 r.,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

KRYTERIA KLASYFIKACJI

Artykuł 1

Klienci, kontrahenci finansowi i transakcje

1. Liczba klientów, których dotyczy incydent, o której mowa w art. 18 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, odzwierciedla liczbę wszystkich klientów, których dotyczy incydent, zarówno osób fizycznych, jak i prawnych, które nie są lub nie były w stanie skorzystać z usługi świadczonej przez podmiot finansowy podczas incydentu lub które odczuły niekorzystne skutki incydentu. Liczba ta uwzględnia również osoby trzecie, które są wyraźnie objęte umową między podmiotem finansowym a klientem w charakterze beneficjentów usługi, której dotyczy incydent.

2. Liczba kontrahentów finansowych, których dotyczy incydent, o której mowa w art. 18 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, odzwierciedla liczbę wszystkich kontrahentów finansowych, których dotyczy incydent, którzy zawarli z podmiotem finansowym ustalenie umowne.

3. W odniesieniu do znaczenia klientów i kontrahentów finansowych, których dotyczy incydent, o którym mowa w art. 18 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, podmiot finansowy bierze pod uwagę stopień, w jakim wpływ incydentu na klienta lub kontrahenta finansowego przełoży się na osiągnięcie celów biznesowych przez podmiot finansowy, a także potencjalny wpływ incydentu na efektywność rynku.

4. W odniesieniu do kwoty lub liczby transakcji, których dotyczy incydent, o których mowa w art. 18 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, podmiot finansowy uwzględnia wszystkie transakcje, których dotyczy incydent, na kwotę pieniężną, w przypadku gdy co najmniej jedna część transakcji jest przeprowadzana w Unii.

5. Jeżeli nie można określić faktycznej liczby klientów lub kontrahentów finansowych, których dotyczy incydent, lub faktycznej liczby lub kwoty transakcji, których dotyczy incydent, podmiot finansowy szacuje te liczby lub kwoty na podstawie dostępnych danych z porównywalnych okresów odniesienia.

Artykuł 2

Skutki reputacyjne

1. Do celów ustalenia skutków reputacyjnych incydentu, o których mowa w art. 18 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, podmioty finansowe uznają, że skutki reputacyjne mają miejsce wówczas, gdy spełnione zostało co najmniej jedno z następujących kryteriów:

a) incydent został opisany w mediach;

b) incydent doprowadził do powtarzających się skarg ze strony różnych klientów lub kontrahentów finansowych dotyczących usług ukierunkowanych na klienta lub krytycznych relacji biznesowych;

c) w wyniku incydentu podmiot finansowy nie będzie w stanie lub prawdopodobnie nie będzie w stanie spełnić wymogów regulacyjnych;

d) w wyniku incydentu podmiot finansowy utraci lub prawdopodobnie utraci klientów lub kontrahentów finansowych, co będzie miało istotny wpływ na jego działalność.

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Oceniając skutki reputacyjne incydentu, podmioty finansowe uwzględniają poziom widoczności, jaką incydent uzyskał lub może uzyskać w odniesieniu do każdego kryterium wymienionego w ust. 1.

Artykuł 3

Czas trwania incydentu i przerwa w świadczeniu usług

1. Podmioty finansowe mierzą czas trwania incydentu, o którym mowa w art. 18 ust. 1 lit. b) rozporządzenia (UE) 2022/2554, od momentu wystąpienia incydentu do momentu jego rozwiązania.

Jeżeli podmioty finansowe nie są w stanie określić momentu wystąpienia incydentu, mierzą czas trwania incydentu od momentu jego wykrycia. W przypadku gdy podmioty finansowe dowiedzą się, że incydent miał miejsce przed jego wykryciem, mierzą czas trwania od momentu zarejestrowania incydentu w dzienniku sieciowym lub systemowym lub w innych źródłach danych.

Jeżeli podmioty finansowe nie wiedzą jeszcze, kiedy incydent zostanie rozwiązany, lub nie są w stanie zweryfikować zapisów w dziennikach lub innych źródłach danych, stosują oszacowania.

2. Podmioty finansowe mierzą przerwę w świadczeniu usługi spowodowaną incydentem, o której mowa w art. 18 ust. 1 lit. b) rozporządzenia (UE) 2022/2554, od momentu gdy usługa staje się w pełni lub częściowo niedostępna dla klientów, kontrahentów finansowych lub innych użytkowników wewnętrznych lub zewnętrznych do momentu przywrócenia regularnych działań lub operacji do poziomu usługi świadczonej przed wystąpieniem incydentu. W przypadku gdy przerwa w świadczeniu usług powoduje opóźnienie w świadczeniu usługi po przywróceniu regularnych działań lub operacji, czas przestoju mierzy się od początku incydentu do momentu, w którym usługa, w przypadku której wystąpiło opóźnienie, jest świadczona w całości.

Jeżeli podmioty finansowe nie są w stanie określić momentu rozpoczęcia przerwy w świadczeniu usług, mierzą czas trwania przerwy w świadczeniu usług od momentu jej wykrycia.

Artykuł 4

Zasięg geograficzny

Do celów ustalenia zasięgu geograficznego w odniesieniu do obszarów, których dotyczy incydent, o którym to zasięgu mowa w art. 18 ust. 1 lit. c) rozporządzenia (UE) 2022/2554, podmioty finansowe oceniają, czy skutki incydentu są lub były odczuwalne w innych państwach członkowskich, a w szczególności oceniają skutki w odniesieniu do:

a) klientów i kontrahentów finansowych w innych państwach członkowskich;

b) oddziałów lub innych podmiotów finansowych należących do grupy prowadzących działalność w innych państwach członkowskich;

c) infrastruktury rynku finansowego lub dostawców będących osobami trzecimi, którzy mogą mieć wpływ na podmioty finansowe w innych państwach członkowskich, na rzecz których świadczą usługi, w zakresie, w jakim takie informacje są dostępne.

Artykuł 5

Utrata danych

Do celów ustalenia utraty danych w wyniku incydentu, o której mowa w art. 18 ust. 1 lit. d) rozporządzenia (UE) 2022/2554, podmioty finansowe uwzględniają następujące kwestie:

a) w odniesieniu do dostępności danych – czy incydent sprawił, że dane, do których dostępu zażądał podmiot finansowy, jego klienci lub jego kontrahenci, stały się tymczasowo lub trwale niedostępne lub nienadające się do wykorzystania;

b) w odniesieniu do autentyczności danych – czy incydent spowodował spadek wiarygodności źródła danych;

c) w odniesieniu do integralności danych – czy incydent spowodował nieupoważnioną modyfikację danych, wskutek której stały się one niedokładne lub niekompletne;

d) w odniesieniu do poufności danych – czy w wyniku incydentu nieupoważniona osoba lub system uzyskały dostęp do danych lub dane zostały im ujawnione.

Artykuł 6

Krytyczność usług, których dotyczy incydent

Do celów ustalenia krytyczności usług, których dotyczy incydent, o której mowa w art. 18 ust. 1 lit. e) rozporządzenia (UE) 2022/2554, podmioty finansowe oceniają, czy incydent:

a) dotyczy lub dotyczył usług ICT lub sieci i systemów informatycznych, które wspierają krytyczne lub istotne funkcje podmiotu finansowego;

b) dotyczy lub dotyczył usług finansowych świadczonych przez podmiot finansowy, które wymagają upoważnienia, rejestracji lub podlegają nadzorowi przez właściwe organy;

c) stanowi lub stanowił skuteczny, złośliwy i nieuprawniony dostęp do sieci i systemów informatycznych podmiotu finansowego.

Artykuł 7

Skutki gospodarcze

1. Do celów ustalenia skutków gospodarczych incydentu, o których mowa w art. 18 ust. 1 lit. f) rozporządzenia (UE) 2022/2554, podmioty finansowe, nie wliczając odzyskanych środków finansowych, uwzględniają następujące rodzaje bezpośrednich i pośrednich kosztów i strat, które poniosły w wyniku incydentu:

a) wywłaszczone środki lub aktywa finansowe, za które są odpowiedzialne, w tym aktywa utracone w wyniku kradzieży;

b) koszty zastąpienia lub przeniesienia oprogramowania, sprzętu lub infrastruktury;

c) koszty personelu, w tym koszty związane z zastąpieniem lub przeniesieniem personelu, rekrutacją dodatkowych pracowników, wynagrodzeniem za godziny nadliczbowe oraz odzyskaniem utraconych lub ograniczonych umiejętności;

d) opłaty z tytułu nieprzestrzegania zobowiązań umownych;

e) koszty poniesione w związku z roszczeniami dochodzonymi przez klientów i wypłaconymi im odszkodowaniami;

f) straty wynikające z utraconych dochodów;

g) koszty związane z komunikacją wewnętrzną i zewnętrzną;

h) koszty doradztwa, w tym koszty związane z doradztwem prawnym, usługami kryminalistycznymi i usługami z zakresu środków zaradczych.

2. Koszty i straty, o których mowa w ust. 1, nie obejmują kosztów niezbędnych do bieżącego prowadzenia działalności, w szczególności:

a) kosztów ogólnej konserwacji infrastruktury, urządzeń, sprzętu i oprogramowania komputerowego oraz kosztów aktualizacji umiejętności personelu;

b) kosztów wewnętrznych ani zewnętrznych służących usprawnieniu działalności po wystąpieniu incydentu, w tym modernizacji, udoskonaleń oraz inicjatyw w zakresie oceny ryzyka;

c) składek ubezpieczeniowych.

3. Podmioty finansowe obliczają kwoty kosztów i strat na podstawie danych dostępnych w momencie zgłoszenia. W przypadku gdy nie można ustalić rzeczywistych kwot kosztów i strat, podmioty finansowe opracowują szacunki tych kwot.

4. Oceniając skutki gospodarcze incydentu, podmioty finansowe sumują koszty i straty, o których mowa w ust. 1.

ROZDZIAŁ II

POWAŻNE INCYDENTY I PROGI ISTOTNOŚCI

Artykuł 8

Poważne incydenty

1. Incydent uznaje się za poważny incydent do celów art. 19 ust. 1 rozporządzenia (UE) 2022/2554, jeżeli dotyczy on usług krytycznych, o których mowa w art. 6, oraz jeżeli spełniony jest którykolwiek z poniższych warunków:

a) osiągnięto próg istotności, o którym mowa w art. 9 ust. 5 lit. b);

b) osiągnięto co najmniej dwa spośród pozostałych progów istotności, o których mowa w art. 9 ust. 1–6.

2. Powtarzające się incydenty, które pojedynczo nie są uznawane za poważny incydent zgodnie z ust. 1, uznaje się za jeden poważny incydent, jeżeli spełniają wszystkie poniższe warunki:

a) wystąpiły co najmniej dwa razy w ciągu 6 miesięcy;

b) mają tę samą widoczną podstawową przyczynę, o której mowa w art. 20 akapit pierwszy lit. b) rozporządzenia (UE) 2022/2554;

c) łącznie spełniają one określone w ust. 1 kryteria uznania ich za poważny incydent.

Podmioty finansowe oceniają występowanie powtarzających się incydentów w ujęciu miesięcznym.

Niniejszy ustęp nie ma zastosowania do mikroprzedsiębiorstw i podmiotów finansowych wymienionych w art. 16 ust. 1 rozporządzenia (UE) 2022/2554.

Artykuł 9

Progi istotności do celów ustalania poważnych incydentów

1. Próg istotności dotyczący kryterium „klienci, kontrahenci finansowi i transakcje” zostaje osiągnięty, jeżeli spełniony jest którykolwiek z poniższych warunków:

a) liczba klientów, których dotyczy incydent, przekracza 10 % wszystkich klientów korzystających z danej usługi;

b) liczba klientów, których dotyczy incydent, korzystających z usługi, której dotyczy incydent, przekracza 100 000;

c) liczba kontrahentów finansowych, których dotyczy incydent, przekracza 30 % wszystkich kontrahentów finansowych prowadzących działania związane ze świadczeniem usługi, której dotyczy incydent;

d) liczba transakcji, których dotyczy incydent, przekracza 10 % średniej dziennej liczby transakcji przeprowadzonych przez podmiot finansowy w związku z usługą, której dotyczy incydent;

e) kwota transakcji, których dotyczy incydent, przekracza 10 % średniej dziennej kwoty transakcji przeprowadzonych przez podmiot finansowy w związku z usługą, której dotyczy incydent;

f) incydent dotyczy klientów lub kontrahentów finansowych, którzy zostali zidentyfikowani jako znaczący zgodnie z art. 1 ust. 3.

Jeżeli nie można określić faktycznej liczby klientów lub kontrahentów finansowych, których dotyczy incydent, lub faktycznej liczby lub kwoty transakcji, których dotyczy incydent, podmiot finansowy szacuje te liczby lub kwoty na podstawie dostępnych danych z porównywalnych okresów odniesienia.

2. Próg istotności dotyczący kryterium „skutki reputacyjne” zostaje osiągnięty, jeżeli spełniony jest którykolwiek warunków określonych w art. 2 lit. a)–d).

3. Próg istotności dotyczący kryterium „czas trwania incydentu i przerwa w świadczeniu usług” zostaje osiągnięty, jeżeli spełniony jest którykolwiek z poniższych warunków:

a) czas trwania incydentu jest dłuższy niż 24 godziny;

b) przerwa w świadczeniu usług wynosi dłużej niż 2 godziny w przypadku usług ICT wspierających krytyczne lub istotne funkcje.

4. Próg istotności dotyczący kryterium „zasięg geograficzny" zostaje osiągnięty, jeżeli skutki incydentu są odczuwalne w co najmniej dwóch państwach członkowskich zgodnie z art. 4.

5. Próg istotności dotyczący kryterium „utrata danych" zostaje osiągnięty, jeżeli spełniony jest którykolwiek z poniższych warunków:

a) którykolwiek ze skutków, o których mowa w art. 5, dla dostępności, autentyczności, integralności lub poufności danych ma lub będzie miał niekorzystny wpływ na osiąganie celów biznesowych podmiotu finansowego lub na jego zdolność do spełnienia wymogów regulacyjnych;

b) do sieci i systemów informatycznych miał miejsce udany, złośliwy i nieuprawniony dostęp nieobjęty lit. a), w przypadku gdy taki dostęp może spowodować utratę danych.

6. Próg istotności dotyczący kryterium „skutki gospodarcze" zostaje osiągnięty, jeżeli koszty i straty poniesione przez podmiot finansowy w wyniku incydentu przekroczyły lub prawdopodobnie przekroczą 100 000 EUR.

ROZDZIAŁ III

ZNACZĄCE CYBERZAGROŻENIA

Artykuł 10

Wysokie progi istotności do celów ustalania znaczących cyberzagrożeń

Do celów art. 18 ust. 2 rozporządzenia (UE) 2022/2554 cyberzagrożenie uznaje się za znaczące, jeżeli spełnione są wszystkie poniższe warunki:

a) cyberzagrożenie – jeżeli dojdzie do jego urzeczywistnienia – może lub mogło dotyczyć krytycznych lub istotnych funkcji podmiotu finansowego lub może dotyczyć innych podmiotów finansowych, dostawców będących osobami trzecimi, klientów lub kontrahentów finansowych, na podstawie informacji dostępnych podmiotowi finansowemu;

b) istnieje duże prawdopodobieństwo urzeczywistnienia się cyberzagrożenia u podmiotu finansowego lub innych podmiotów finansowych, biorąc pod uwagę co najmniej następujące elementy:

   (i) mające zastosowanie ryzyka związane z cyberzagrożeniem, o którym mowa w lit. a), w tym potencjalne słabości systemów podmiotu finansowego, które można wykorzystać;

   (ii) zdolności i zamiary agresorów w zakresie znanym podmiotowi finansowemu;

   (iii) utrzymywanie się zagrożenia oraz wszelkie zgromadzone informacje na temat incydentów, które miały wpływ na podmiot finansowy lub jego dostawcę będącego osobą trzecią, klientów lub kontrahentów finansowych;

c) cyberzagrożenie – jeżeli dojdzie do jego urzeczywistnienia – może spełniać którekolwiek z poniższych kryteriów:

   (i) kryterium dotyczące krytyczności usług określone w art. 18 ust. 1 lit. e) rozporządzenia (UE) 2022/2554, jak określono w art. 6 niniejszego rozporządzenia;

   (ii) próg istotności określony w art. 9 ust. 1;

   (iii) próg istotności określony w art. 9 ust. 4.

Jeżeli w zależności od rodzaju cyberzagrożenia i dostępnych informacji podmiot finansowy stwierdzi, że progi istotności określone w art. 9 ust. 2, 3, 5 i 6 mogą zostać osiągnięte, progi te można również uwzględnić.

ROZDZIAŁ IV

ZNACZENIE POWAŻNYCH INCYDENTÓW DLA WŁAŚCIWYCH ORGANÓW W INNYCH PAŃSTWACH CZŁONKOWSKICH ORAZ SZCZEGÓŁOWE INFORMACJE DOTYCZĄCE ZGŁASZANIA, KTÓRE MAJĄ BYĆ UDOSTĘPNIANE WŁAŚCIWYM ORGANOM

Artykuł 11

Znaczenie poważnych incydentów dla właściwych organów w innych państwach członkowskich

Podstawę oceny, czy poważny incydent jest istotny dla właściwych organów w innych państwach członkowskich, o których mowa w art. 19 ust. 7 rozporządzenia (UE) 2022/2554, stanowi fakt, czy podstawowa przyczyna incydentu pochodzi z innego państwa członkowskiego lub czy incydent ma lub miał znaczący wpływ w innym państwie członkowskim na którekolwiek z poniższych podmiotów lub elementów:

a) klientów lub kontrahentów finansowych;

b) oddział podmiotu finansowego lub inny podmiot finansowy należący do grupy;

c) infrastrukturę rynku finansowego lub dostawcę będącego osobą trzecią, który może mieć wpływ na podmioty finansowe, na rzecz których świadczy usługi.

Artykuł 12

Szczegółowe informacje dotyczące poważnych incydentów, które mają być udostępniane właściwym organom

Szczegółowe informacje dotyczące poważnych incydentów, które mają być przekazywane przez właściwe organy innym właściwym organom zgodnie z art. 19 ust. 6 rozporządzenia (UE) 2022/2554, oraz powiadomienia, które mają być przekazywane przez EUNB, ESMA lub EIOPA i EBC odpowiednim właściwym organom w innych państwach członkowskich zgodnie z art. 19 ust. 7 tego rozporządzenia, zawierają taki sam poziom informacji, bez anonimizacji, co powiadomienia i zgłoszenia dotyczące poważnych incydentów otrzymane od podmiotów finansowych zgodnie z art. 19 ust. 4 rozporządzenia (UE) 2022/2554.

ROZDZIAŁ V

PRZEPISY KOŃCOWE

Artykuł 13

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 13 marca 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN