ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2025/1190

z dnia 13 lutego 2025 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria stosowane do identyfikacji podmiotów finansowych zobowiązanych do przeprowadzania testów penetracyjnych pod kątem wyszukiwania zagrożeń, wymogi i standardy regulujące korzystanie z testerów wewnętrznych, wymogi dotyczące zakresu, metodyki testowania i podejścia dla każdego etapu procesu testowania oraz etapów testów odnoszących się do wyników, zamykania i środków naprawczych, a także rodzaj współpracy w zakresie nadzoru i inne odpowiednie rodzaje współpracy potrzebne do przeprowadzenia TLPT i do ułatwienia wzajemnego uznawania

(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. 26 ust. 11 akapit trzeci,

a także mając na uwadze, co następuje:

(1) Niniejsze rozporządzenie zostało opracowane zgodnie z ramami TIBER-EU i odzwierciedla metodykę, proces i strukturę testów penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT) opisanych w TIBER-EU. Podmioty finansowe podlegające obowiązkowi przeprowadzania TLPT mogą odwoływać się do ram TIBER-EU lub krajowych przepisów wdrażających te ramy i stosować te ramy lub przepisy, o ile są one zgodne z wymogami określonymi w art. 26 i 27 rozporządzenia (UE) 2022/2554 oraz w niniejszym rozporządzeniu. Wyznaczenie jednego organu publicznego w sektorze finansowym odpowiedzialnego na poziomie krajowym za kwestie związane z TLPT zgodnie z art. 26 ust. 9 rozporządzenia (UE) 2022/2554 powinno pozostawać bez uszczerbku dla kompetencji właściwych organów w zakresie nadzoru nad niektórymi podmiotami finansowymi powierzonych na poziomie Unii – zgodnie z art. 46 tego rozporządzenia – organom takim jak na przykład Europejski Bank Centralny w odniesieniu do istotnych instytucji kredytowych, które to organy należy uznać za właściwe w kwestiach związanych z TLPT. W przypadku gdy tylko niektóre zadania związane z TLPT są przekazywane innemu organowi krajowemu w sektorze finansowym na podstawie art. 26 ust. 10 rozporządzenia (UE) 2022/2554, organem właściwym dla zadań związanych z TLPT, które nie zostały przekazane, powinien nadal być właściwy organ w odniesieniu do danego podmiotu finansowego wskazany w art. 46 tego rozporządzenia.

(2) Biorąc pod uwagę złożoność TLPT i związane z nimi ryzyko, ich stosowanie powinno być ograniczone do tych podmiotów finansowych, w przypadku których jest to uzasadnione. W związku z tym organy odpowiedzialne za kwestie związane z TLPT (organy ds. TLPT na szczeblu unijnym albo krajowym) powinny wyłączyć z zakresu TLPT te podmioty finansowe, które działają w podsektorach podstawowych usług finansowych, w przypadku których przeprowadzanie TLPT nie jest uzasadnione. Oznacza to, że instytucje kredytowe, instytucje płatnicze i instytucje pieniądza elektronicznego, centralne depozyty papierów wartościowych, kontrahenci centralni, systemy obrotu, zakłady ubezpieczeń i zakłady reasekuracji, mimo że spełniają kryteria ilościowe, mogą zostać zwolnione z wymogu przeprowadzania TLPT w świetle ogólnej oceny ich profilu ryzyka związanego z ICT i zaawansowania pod względem ICT, wpływu na sektor finansowy i związanych z tym kwestii dotyczących stabilności finansowej.

(3) Organy ds. TLPT powinny ocenić – w świetle ogólnej oceny profilu ryzyka związanego z ICT i zaawansowania pod względem ICT, wpływu na sektor finansowy oraz związanych z tym kwestii dotyczących stabilności finansowej – czy któryś rodzaj podmiotu finansowego inny niż instytucje kredytowe, instytucje płatnicze, instytucje pieniądza elektronicznego, kontrahenci centralni, centralne depozyty papierów wartościowych, systemy obrotu, zakłady ubezpieczeń i zakłady reasekuracji powinien podlegać obowiązkowi przeprowadzania TLPT. Ocena, czy takie podmioty finansowe spełniają wspomniane kryteria jakościowe, powinna służyć określeniu – przy użyciu obiektywnych wskaźników międzysektorowych – podmiotów finansowych, dla których przeprowadzanie TLPT jest właściwe. Jednocześnie ocena, czy podmiot finansowy spełnia te kryteria jakościowe, powinna ograniczyć podmioty

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

objęte TLPT do tych, dla których przeprowadzenie testów jest uzasadnione. To, czy podmiot finansowy spełnia te kryteria jakościowe, należy również oceniać w świetle rozwoju nowych rynków i rosnącego znaczenia dla sektora finansowego w przyszłości nowych uczestników rynku, w tym dostawców usług w zakresie kryptoaktywów, którzy uzyskali zezwolenie zgodnie z art. 59 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 ([2]).

(4) Podmioty finansowe mogą mieć tego samego dostawcę usług ICT wewnątrz grupy lub mogą należeć do tej samej grupy i korzystać ze wspólnych systemów ICT. W takim przypadku ważne jest, aby dokonując oceny, czy podmiot finansowy powinien podlegać obowiązkowi przeprowadzania TLPT oraz czy TLPT powinny być przeprowadzane na poziomie podmiotu czy na poziomie grupy (w ramach wspólnych TLPT), organy ds. TLPT brały pod uwagę strukturę tego podmiotu finansowego i jego systemowy charakter lub znaczenie dla sektora finansowego na poziomie krajowym lub unijnym.

(5) Aby odzwierciedlać ramy TIBER-EU, w metodyce testowania należy przewidzieć zaangażowanie następujących głównych uczestników: podmiotu finansowego, wraz z zespołem typu control team (odpowiadającym zespołowi typu control team w TIBER-EU) i zespołem typu blue team (odpowiadającym zespołowi typu blue team w TIBER-EU), oraz organu ds. TLPT, w postaci zespołu typu TLPT cyber team (odpowiadającego zespołowi typu TIBER cyber team w TIBER-EU), a także dostawcę analizy zagrożeń i testerów (przy czym testerzy odpowiadają dostawcy zespołu typu red team w TIBER-EU).

(6) W celu zapewnienia, aby podczas TLPT wykorzystano doświadczenia zdobyte w ramach wdrażania TIBER-EU, oraz w celu zmniejszenia ryzyka związanego z przeprowadzaniem TLPT należy zapewnić, aby obowiązki zespołów typu TLPT cyber team, które mają zostać ustanowione na poziomie organów ds. TLPT, jak najściślej odpowiadały obowiązkom zespołów typu cyber team w TIBER-EU. W związku z tym zespoły typu TLPT cyber team powinny mieć kierowników testów, którzy będą odpowiedzialni za nadzorowanie poszczególnych TLPT oraz za ich planowanie i koordynację. Zespoły typu TLPT cyber team powinny pełnić rolę pojedynczego punktu kontaktowego na potrzeby przekazywania wewnętrznym i zewnętrznym zainteresowanym stronom informacji dotyczących testów, gromadzenia i przetwarzania informacji zwrotnych i wniosków wyciągniętych z wcześniej przeprowadzonych testów oraz wspierania podmiotów finansowych poddawanych TLPT.

(7) Aby naśladować metodykę ram TIBER-EU, kierownicy testów powinni posiadać umiejętności i zdolności niezbędne do zapewniania doradztwa i kwestionowania propozycji testerów. Z doświadczenia zdobytego w ramach TIBER-EU wynika, że do każdego testu warto przydzielić co najmniej dwóch kierowników testów. Aby odzwierciedlić fakt, że celem TLPT jest zachęcanie do wyciągania wniosków, oraz aby chronić poufność testów, zdecydowanie zaleca się organom ds. TLPT, o ile nie brakuje im personelu lub ekspertów, aby na czas trwania TLPT kierownicy testów nie prowadzili działań nadzorczych w stosunku do tego samego podmiotu finansowego, który jest poddawany TLPT.

(8) Dla zachowania spójności z ramami TIBER-EU ważne jest, aby organ ds. TLPT uważnie śledził testowanie na każdym z jego etapów. Biorąc pod uwagę charakter testów i związane z nimi ryzyko, zasadnicze znaczenie ma zaangażowanie organu ds. TLPT w każdy konkretny etap testów. W szczególności należy konsultować z organem ds. TLPT i poddawać zatwierdzeniu przez niego te oceny lub decyzje podmiotów finansowych, które mogą z jednej strony wpływać na skuteczność testu, a z drugiej strony mieć wpływ na ryzyko związane z testem. Podstawowe kroki, w odniesieniu do których konieczne jest szczególne zaangażowanie organu ds. TLPT, obejmują zatwierdzanie niektórych podstawowych dokumentów dotyczących testów, a także wybór dostawców analizy zagrożeń i testerów oraz środków zarządzania ryzykiem. Zaangażowanie organów ds. TLPT, w szczególności w przypadku zatwierdzania, nie powinno skutkować nadmiernym obciążeniem dla tych organów, a zatem powinno być ograniczone do tych dokumentów i decyzji, które mają bezpośredni wpływ na przeprowadzanie TLPT. Dzięki aktywnemu udziałowi w każdej fazie testów organy ds. TLPT mogą skutecznie ocenić spełnianie przez podmioty finansowe odpowiednich wymogów, co powinno umożliwić tym organom wydawanie poświadczeń zgodnie z art. 26 ust. 7 rozporządzenia (UE) 2022/2554.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U. L 150 z 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Poufność TLPT ma ogromne znaczenie dla zapewnienia realistycznych warunków testowania. Z tego powodu testy powinny być niejawne i należy wprowadzić środki ostrożności w celu zachowania ich poufności, w tym nadając TLPT kryptonimy, które powinny być skonstruowane w taki sposób, aby uniemożliwić identyfikację TLPT przez osoby trzecie. Gdyby pracownicy odpowiedzialni za bezpieczeństwo podmiotu finansowego byli świadomi planowanych lub trwających TLPT, istnieje prawdopodobieństwo, że byliby bardziej uważni i czujni niż w normalnych warunkach pracy, co skutkowałoby zmienionym wynikiem testów. Pracownicy podmiotu finansowego nienależący do zespołu typu control team powinni być zatem informowani o wszelkich planowanych lub trwających TLPT tylko wtedy, gdy istnieją ku temu uzasadnione powody, i z zastrzeżeniem uprzedniej zgody kierowników testów, między innymi w celu zapewnienia tajności testu w przypadku wykrycia testowania przez członka zespołu typu blue team.

(10) Jak wynika z doświadczeń zgromadzonych w ramach TIBER-EU w odniesieniu do zespołu typu control team, do bezpiecznego przeprowadzenia TLPT niezbędny jest wybór odpowiedniego lidera zespołu typu control team. Lider zespołu typu control team powinien być odpowiednio upoważniony przez podmiot finansowy do kierowania wszystkimi aspektami testów, bez narażania ich poufności. Z tego samego powodu członkowie zespołu typu control team powinni dysponować dogłębną wiedzą na temat podmiotu finansowego, roli lidera zespołu typu control team i jego strategicznej pozycji, powinni mieć odpowiednie starszeństwo służbowe oraz powinni mieć dostęp do zarządu. Aby ograniczyć ryzyko niepowodzenia TLPT, zespół typu control team powinien być jak najmniejszy.

(11) TLPT wiążą się z nieodłącznymi elementami ryzyka, ponieważ krytyczne funkcje są testowane w działającym na bieżąco środowisku produkcyjnym, co może powodować incydenty odmowy dostępu, nieoczekiwane awarie systemu, uszkodzenia działających na bieżąco krytycznych systemów produkcyjnych lub utratę, modyfikację bądź ujawnienie danych. Zagrożenia te uwydatniają potrzebę stosowania solidnych środków zarządzania ryzykiem. W celu zapewnienia, aby TLPT były przeprowadzane w sposób kontrolowany przez cały czas ich trwania, bardzo ważne jest, aby podmioty finansowe były w każdym momencie świadome szczególnego ryzyka, które występuje w przypadku TLPT, oraz aby ryzyko to było ograniczane. W tym względzie, bez uszczerbku dla wewnętrznych procesów podmiotu finansowego oraz odpowiedzialności i uprawnień już przekazanych liderowi zespołu typu control team, zasadne może być informowanie o środkach zarządzania ryzykiem związanym TLPT lub, w szczególnych przypadkach, zatwierdzenie tych środków zarządzania ryzykiem przez sam organ zarządzający podmiotu finansowego. W celu zmniejszenia tego ryzyka oraz zapewnienia, by specjalistyczne usługi świadczone przez testerów i dostawców analizy zagrożeń (zwanych łącznie „dostawcami TLPT") były najwyższej jakości, niezbędne jest również, aby odznaczali się oni najwyższym poziomem umiejętności, wiedzy fachowej i odpowiednim doświadczeniem w zakresie analizy zagrożeń i TLPT w branży usług finansowych.

(12) Konwencjonalne testy penetracyjne pozwalają na szczegółową i użyteczną ocenę podatności technicznych i konfiguracyjnych często pojedynczego systemu lub wydzielonego środowiska, ale w przeciwieństwie do opartych na analizie zagrożeń testów z udziałem zespołu typu red team nie obejmują pełnego scenariusza ukierunkowanego ataku na cały podmiot, w tym wszystkich jego pracowników, wszystkie procesy i technologie. Dokonując wyboru dostawców TLPT, podmioty finansowe powinny zatem zapewnić, aby dostawcy ci posiadali umiejętności wymagane do przeprowadzania opartych na analizie zagrożeń testów z udziałem zespołu typu red team, a nie tylko testów penetracyjnych. Konieczne jest zatem ustanowienie kompleksowych kryteriów dla testerów, zarówno wewnętrznych, jak i zewnętrznych, oraz dostawców analizy zagrożeń, zawsze zewnętrznych. W przypadku gdy dostawcy TLPT należą do tego samego przedsiębiorstwa, należy odpowiednio oddzielić pracowników wyznaczonych do TLPT.

(13) W wyjątkowych okolicznościach podmioty finansowe mogą nie być w stanie zawrzeć umowy z dostawcami TLPT spełniającymi wspomniane kompleksowe kryteria. Po udowodnieniu niedostępności takich dostawców analizy zagrożeń podmioty finansowe powinny mieć zatem możliwość zaangażowania osób, które nie spełniają wszystkich kompleksowych kryteriów, pod warunkiem że odpowiednio ograniczą one wszelkie wynikające z tego dodatkowe ryzyko oraz że organ ds. TLPT dokona oceny wszystkich tych kryteriów.

(14) W przypadku gdy w TLPT zaangażowanych jest kilka podmiotów finansowych i kilka organów ds. TLPT, w celu przeprowadzenia jak najbardziej efektywnych i bezpiecznych testów należy określić role wszystkich stron w procesie TLPT. Na potrzeby testowania zbiorczego konieczne jest wprowadzenie szczegółowych wymogów określających rolę wyznaczonego podmiotu finansowego, a mianowicie, że powinien on być odpowiedzialny za dostarczenie całej niezbędnej dokumentacji wiodącemu organowi ds. TLPT oraz za monitorowanie procesu testowania. Wyznaczony podmiot finansowy powinien również odpowiadać za wspólne aspekty oceny zarządzania ryzykiem. Niezależnie od roli wyznaczonego podmiotu finansowego obowiązki każdego podmiotu finansowego uczestniczącego w procesie zbiorczego TLPT powinny pozostać niezmienione podczas testu zbiorczego. Ta sama zasada powinna mieć zastosowanie do wspólnych TLPT.

(15) Jak pokazują doświadczenia z wdrażania ram TIBER-EU, najskuteczniejszym sposobem zapewnienia, aby testy były przeprowadzane we właściwy sposób, jest organizowanie stacjonarnych lub wirtualnych spotkań z udziałem wszystkich zainteresowanych stron (podmiotów finansowych, organów, testerów i dostawców analizy zagrożeń). Takie stacjonarne i wirtualne spotkania powinny zatem odbywać się na różnych etapach procesu, a w szczególności na etapie przygotowawczym podczas uruchomienia TLPT w celu ostatecznego ustalenia ich zakresu, na etapie testowania w celu sfinalizowania sprawozdania z analizy zagrożeń i planu testów z udziałem zespołu typu red team oraz w celu dokonywania cotygodniowych aktualizacji, a także na etapie zamykania testów w celu odtworzenia działań testerów i zespołu typu blue team, działań z udziałem zespołu typu purple team i wymiany informacji zwrotnych na temat TLPT.

(16) Aby zapewnić sprawne przeprowadzanie TLPT, organ ds. TLPT powinien jasno przedstawić podmiotowi finansowemu swoje oczekiwania dotyczące testowania. W związku z tym kierownicy testów powinni zapewnić odpowiedni przepływ informacji do zespołu typu control team w ramach podmiotu finansowego oraz do dostawców TLPT.

(17) Podmiot finansowy powinien wybrać krytyczne lub istotne funkcje, które będą objęte zakresem TLPT. Przy wyborze tych funkcji podmiot finansowy powinien opierać się na różnych kryteriach dotyczących znaczenia każdej funkcji dla samego podmiotu finansowego i dla sektora finansowego, na szczeblu unijnym i krajowym, nie tylko pod względem gospodarczym, ale również z uwzględnieniem symbolicznego lub politycznego statusu tej funkcji. Aby ułatwić płynne przejście do etapu gromadzenia danych na potrzeby analizy zagrożeń, zespół typu control team powinien przekazać testerom i dostawcy analizy zagrożeń, którzy nie są zaangażowani w proces ustalania zakresu, szczegółowe informacje na temat uzgodnionego zakresu.

(18) Aby zapewnić testerom informacje potrzebne do symulacji rzeczywistego i realistycznego ataku na działające na bieżąco systemy podmiotu finansowego stanowiące podstawę jego krytycznych lub istotnych funkcji, dostawca analizy zagrożeń powinien gromadzić dane lub informacje dotyczące co najmniej dwóch kluczowych obszarów zainteresowania: celów, poprzez zidentyfikowanie potencjalnych powierzchni ataku w całym podmiocie finansowym, oraz zagrożeń, poprzez zidentyfikowanie odnośnych agresorów i prawdopodobnych scenariuszy zagrożeń. W celu zapewnienia, aby dostawca analizy zagrożeń uwzględnił zagrożenia istotne dla podmiotu finansowego, testerzy, zespół typu control team i kierownicy testów powinni udzielić mu informacji zwrotnej na temat projektu sprawozdania z analizy zagrożeń. Jako punkt odniesienia dla krajowego krajobrazu zagrożeń dostawca analizy zagrożeń może wykorzystać ogólny krajobraz zagrożeń stworzony przez organ ds. TLPT dla sektora finansowego danego państwa członkowskiego, o ile jest on dostępny. Jak wynika ze stosowania ram TIBER-EU, proces gromadzenia informacji na potrzeby analizy zagrożeń trwa zazwyczaj około 4 tygodni.

(19) Aby umożliwić testerom uzyskanie szczegółowych informacji i dalszy przegląd dokumentu określającego zakres i sprawozdania z ukierunkowanej analizy zagrożeń w celu sfinalizowania planu testów z udziałem zespołu typu red team, ważne jest, aby przed etapem testowania TLPT z udziałem zespołu typu red team testerzy otrzymali od dostawcy analizy zagrożeń szczegółowe wyjaśnienia dotyczące sprawozdania z ukierunkowanej analizy zagrożeń i analizy możliwych scenariuszy zagrożeń.

(20) Aby umożliwić testerom przeprowadzenie realistycznych i kompleksowych testów, w ramach których przeprowadzane są wszystkie etapy ataku i osiągane są flagi, należy przydzielić wystarczająco dużo czasu na etap aktywnego testowania z udziałem zespołu typu red team. Z doświadczeń z ramami TIBER-EU wynika, że czas ten powinien wynosić co najmniej 12 tygodni i powinien on zostać określony z uwzględnieniem liczby zaangażowanych stron, zakresu TLPT, zasobów zaangażowanego podmiotu finansowego lub zaangażowanych podmiotów finansowych, wszelkich wymogów zewnętrznych oraz dostępności informacji uzupełniających dostarczonych przez podmiot finansowy.

(21) Podczas etapu aktywnego testowania z udziałem zespołu typu red team testerzy powinni stosować szereg taktyk, technik i procedur w celu odpowiedniego przetestowania działających na bieżąco systemów produkcyjnych podmiotu finansowego. Taktyki, techniki i procedury powinny obejmować, w stosownych przypadkach, rozpoznanie (tj. zgromadzenie jak największej ilości informacji na temat celu), zbrojenie (tj. analizę informacji na temat infrastruktury, obiektów i pracowników oraz przygotowanie się do operacji właściwych dla danego celu), realizację (tj. aktywne rozpoczęcie pełnej operacji w odniesieniu do celu), exploity (tj. działania testerów, których celem jest naruszenie integralności serwerów, sieci podmiotu finansowego i wykorzystanie jego personelu poprzez inżynierię społeczną), kontrolę i przemieszczanie się (tj. próby przejścia od systemów, których integralność została naruszona, do systemów bardziej podatnych na zagrożenia lub systemów o wysokiej wartości) oraz działania dotyczące celów (tj. uzyskanie dalszego dostępu do systemów, których integralność została naruszona, i uzyskanie dostępu do wcześniej uzgodnionych informacji i danych dotyczących celów, zgodnie z wcześniejszymi ustaleniami w planie testów z udziałem zespołu typu red team).

(22) Przeprowadzając TLPT, tester powinien działać z uwzględnieniem czasu dostępnego na przeprowadzenie ataku, zasobów oraz granic etycznych i prawnych. Jeżeli testerzy nie są w stanie przejść do kolejnego zaplanowanego etapu ataku, zespół typu control team powinien, za zgodą organu ds. TLPT, zapewnić im okazjonalną pomoc w postaci „ułatwień". Ułatwienia można ogólnie podzielić na ułatwienia w postaci informacji i ułatwienia w postaci dostępu i mogą one polegać na zapewnieniu dostępu do systemów ICT lub sieci wewnętrznych w celu kontynuowania testów i skupienia się na kolejnych etapach ataku.

(23) Podczas etapu aktywnego testowania z udziałem zespołu typu red team – jeśli jest to konieczne, aby umożliwić kontynuację TLPT – w wyjątkowych okolicznościach i po wyczerpaniu wszystkich alternatywnych opcji w ostateczności należy zastosować wspólne testowanie, które obejmuje zarówno testerów, jak i zespół typu blue team. W kontekście takich ograniczonych działań z udziałem zespołu typu purple team można stosować następujące metody: „złap i wypuść", w przypadku których testerzy próbują realizować scenariusze, dają się wykryć, a następnie wznawiają testowanie, „gry wojenne", które umożliwiają bardziej złożone scenariusze testowania strategicznego procesu decyzyjnego, lub „wspólny dowód słuszności koncepcji", który umożliwia testerom i członkom zespołu typu blue team wspólne zatwierdzanie konkretnych środków bezpieczeństwa, narzędzi lub technik w kontrolowanym i opartym na współpracy środowisku.

(24) TLPT powinny być wykorzystywane jako doświadczenie umożliwiające wyciągniecie wniosków z myślą o zwiększeniu operacyjnej odporności cyfrowej podmiotów finansowych. W związku z tym zespół typu blue team i testerzy powinni odtworzyć atak i przeanalizować podjęte kroki, aby wyciągnąć wnioski z doświadczenia testowego przeprowadzonego we współpracy z testerami. W tym celu oraz aby umożliwić odpowiednie przygotowanie, przed podjęciem jakichkolwiek działań związanych z odtwarzaniem ataku należy udostępnić wszystkim stronom biorącym udział w odtwarzaniu sprawozdanie z testu sporządzone przez zespół typu red team oraz sprawozdanie z testu sporządzone przez zespół typu blue team. Ponadto na etapie zamykania należy przeprowadzić działania z udziałem zespołu typu purple team, aby zmaksymalizować doświadczenie edukacyjne. Metody, które można wykorzystać w działaniach z udziałem zespołu typu purple team na etapie zamykania, powinny obejmować dyskusje na temat alternatywnych scenariuszy ataków, zastosowanie w działających na bieżąco systemach scenariuszy alternatywnych lub ponowne zastosowanie w działających na bieżąco systemach zaplanowanych scenariuszy, których testerzy nie byli w stanie ukończyć lub zrealizować na etapie testowania.

(25) Aby jeszcze bardziej ułatwić wszystkim stronom zaangażowanym w TLPT zdobywanie wiedzy – na potrzeby przyszłych testów oraz w celu zwiększenia operacyjnej odporności cyfrowej podmiotów finansowych – zainteresowane strony powinny przekazywać sobie nawzajem informacje zwrotne na temat całego procesu, a w szczególności określać, które działania przebiegły dobrze, a które można by ulepszyć, oraz które aspekty procesu TLPT sprawdziły się, a które można dopracować.

(26) Właściwe organy, o których mowa w art. 46 rozporządzenia (UE) 2022/2554, oraz organy ds. TLPT, jeżeli nie są to te same organy, powinny ze sobą współpracować w celu włączenia do istniejących procesów nadzorczych zaawansowanych testów w postaci TLPT. W związku z tym oraz w celu wspólnego prawidłowego rozumienia ustaleń wynikających z TLPT i sposobu ich interpretacji właściwe jest – w szczególności w odniesieniu do sprawozdania podsumowującego z testów i planów działań naprawczych – nawiązanie ścisłej współpracy między kierownikami testów, którzy byli zaangażowani w TLPT, a odpowiedzialnymi organami nadzoru.

(27) W art. 26 ust. 8 akapit pierwszy rozporządzenia (UE) 2022/2554 nałożono na podmioty finansowe wymóg zlecania co trzeciego testu testerom zewnętrznym. W przypadku gdy podmioty finansowe włączają do zespołu testerów zarówno testerów wewnętrznych, jak i zewnętrznych, do celów tego artykułu należy uznać takie TLPT za przeprowadzone z udziałem testerów wewnętrznych.

(28) Podstawę niniejszego rozporządzenia stanowi projekt regulacyjnych standardów technicznych przedłożony Komisji przez Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (Europejskie Urzędy Nadzoru), w porozumieniu z Europejskim Bankiem Centralnym.

(29) Europejskie Urzędy Nadzoru przeprowadziły otwarte konsultacje publiczne na temat projektu regulacyjnych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, dokonały analizy potencjalnych powiązanych kosztów i korzyści oraz zwróciły się o opinię do Bankowej Grupy Interesariuszy powołanej zgodnie z art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([3]), do Grupy Interesariuszy z Sektora Ubezpieczeń i Reasekuracji oraz Grupy Interesariuszy z Sektora Pracowniczych Programów Emerytalnych powołanych zgodnie z art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1094/2010 ([4]) oraz do Grupy Interesariuszy z Sektora Giełd i Papierów Wartościowych powołanej zgodnie z art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([5]).

(30) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 20 sierpnia 2024 r.,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „zespół typu control team" oznacza zespół złożony z pracowników testowanego podmiotu finansowego oraz, w stosownych przypadkach wynikających z zakresu TLPT, pracowników jego zewnętrznych dostawców usług i wszelkich innych stron, który to zespół zarządza testem;

2) „lider zespołu typu control team" oznacza pracownika podmiotu finansowego odpowiedzialnego za prowadzenie wszystkich działań związanych z TLPT dla podmiotu finansowego w kontekście danego testu;

3) „zespół typu blue team" oznacza pracowników podmiotu finansowego oraz, w stosownych przypadkach, pracowników zewnętrznych dostawców usług podmiotu finansowego i wszelkich innych stron uznanych za istotne z uwagi na zakres TLPT, którzy poprzez utrzymywanie poziomu bezpieczeństwa tego podmiotu finansowego chronią korzystanie przez niego z sieci i systemów informatycznych przed symulowanymi lub rzeczywistymi atakami i którzy nie są świadomi TLPT;

4) „zadania zespołu typu blue team" oznaczają zadania, które są zazwyczaj wykonywane przez zespół typu blue team, takie jak zapewnianie centrum monitorowania bezpieczeństwa (SOC), usługi w zakresie infrastruktury ICT, usługi wsparcia technicznego, usługi zarządzania incydentami na szczeblu operacyjnym;

5) „zespół typu red team" oznacza testerów wewnętrznych lub zewnętrznych, zatrudnionych lub wyznaczonych na potrzeby TLPT;

6) „działania z udziałem zespołu typu purple team" oznacza wspólne działania testowe, które obejmują zarówno testerów, jak i zespół typu blue team;

([3]) 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).

([4]) 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).

([5]) 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).

([6]) 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).

7) „organ ds. TLPT” oznacza którykolwiek z poniższych:

   a) jeden organ publiczny w sektorze finansowym wyznaczony zgodnie z art. 26 ust. 9 rozporządzenia (UE) 2022/2554;

   b) organ w sektorze finansowym, któremu przekazano wykonywanie niektórych lub wszystkich zadań związanych z TLPT zgodnie z art. 26 ust. 10 rozporządzenia (UE) 2022/2554;

   c) każdy z właściwych organów, o których mowa w art. 46 rozporządzenia (UE) 2022/2554;

8) „zespół typu TLPT cyber team” lub „zespół TCT” oznacza personel organów ds. TLPT odpowiedzialny za kwestie związane z TLPT;

9) „kierownicy testów” oznaczają pracowników wyznaczonych do prowadzenia działań organu ds. TLPT w odniesieniu do konkretnych TLPT w celu monitorowania zgodności z niniejszym rozporządzeniem;

10) „dostawca analizy zagrożeń” oznacza ekspertów, z którymi podmiot finansowy zawiera umowę na każde TLPT i którzy są zewnętrzni w stosunku do podmiotu finansowego i dostawców usług ICT wewnątrz grupy, jeśli tacy istnieją, oraz którzy gromadzą i analizują ukierunkowane informacje z analizy zagrożeń istotne dla podmiotów finansowych w zakresie konkretnego procesu TLPT oraz opracowują odpowiednie i realistyczne scenariusze zagrożeń;

11) „dostawcy TLPT” oznaczają testerów i dostawców analizy zagrożeń;

12) „ułatwienie” oznacza pomoc lub informacje dostarczane testerom przez zespół typu control team w celu umożliwienia im dalszej realizacji ścieżki ataku, jeżeli nie są oni w stanie samodzielnie przejść dalej i gdy nie istnieje żadna inna rozsądna alternatywa, w tym ze względu na niewystarczający czas lub niewystarczające zasoby przeznaczone na dane TLPT;

13) „ścieżka ataku” oznacza trasę pokonywaną przez testerów podczas etapu aktywnego testowania TLPT z udziałem zespołu typu red team, aby zdobyć flagi określone dla tych TLPT;

14) „flagi” to kluczowe cele w systemach ICT wspierających krytyczne lub istotne funkcje podmiotu finansowego, do których testerzy próbują dotrzeć podczas testu;

15) „informacje szczególnie chronione” oznaczają informacje, które można z łatwością wykorzystać do przeprowadzania ataków na systemy ICT podmiotu finansowego, własność intelektualną, poufne dane handlowe lub dane osobowe, które mogą bezpośrednio lub pośrednio zaszkodzić podmiotowi finansowemu i jego ekosystemowi, gdyby znalazły się w rękach złośliwych podmiotów;

16) „grupa” oznacza wszystkie podmioty finansowe uczestniczące w zbiorczych TLPT zgodnie z art. 26 ust. 4 rozporządzenia (UE) 2022/2554;

17) „przyjmujące państwo członkowskie” oznacza przyjmujące państwo członkowskie zgodnie z unijnym prawem sektorowym mającym zastosowanie do każdego podmiotu finansowego;

18) „wspólne TLPT” oznaczają TLPT inne niż zbiorcze TLPT, o których mowa w art. 26 ust. 4 rozporządzenia (UE) 2022/2554, obejmujące kilka podmiotów finansowych korzystających z tego samego dostawcy usług ICT wewnątrz grupy lub należących do tej samej grupy i współdzielących systemy ICT.

Artykuł 2

Określanie podmiotów finansowych zobowiązanych do przeprowadzenia TLPT

1. Organy ds. TLPT oceniają, czy dany podmiot finansowy jest zobowiązany do przeprowadzenia TLPT, biorąc pod uwagę wpływ tego podmiotu finansowego, jego systemowy charakter i jego profil ryzyka związanego z ICT, w oparciu o wszystkie poniższe kryteria:

a) czynniki związane z wpływem i systemowym charakterem:

   (i) wielkość podmiotu finansowego, określona na podstawie tego, czy podmiot finansowy świadczy usługi finansowe w jednym państwie członkowskim czy w większej ich liczbie, oraz poprzez porównanie działalności podmiotu finansowego z działalnością innych podmiotów finansowych świadczących podobne usługi;

   (ii) zakres i charakter wzajemnych powiązań danego podmiotu finansowego z innymi podmiotami finansowymi w sektorze finansowym w co najmniej jednym państwie członkowskim;

   (iii) krytyczny lub istotny charakter usług świadczonych przez podmiot finansowy na rzecz sektora finansowego;

(iv) zastępowalność usług świadczonych przez podmiot finansowy;

(v) złożoność modelu biznesowego podmiotu finansowego oraz powiązanych usług i procesów;

(vi) to, czy podmiot finansowy należy do grupy o systemowym charakterze na szczeblu unijnym lub krajowym w sektorze finansowym i czy dzieli z tą grupą systemy ICT;

b) czynniki ryzyka związanego z ICT:

(i) profil ryzyka podmiotu finansowego;

(ii) krajobraz zagrożeń podmiotu finansowego;

(iii) stopień zależności krytycznych lub istotnych funkcji podmiotu finansowego lub jego funkcji wspierających od systemów i procesów ICT;

(iv) złożoność architektury ICT podmiotu finansowego;

(v) usługi i funkcje ICT wspierane przez zewnętrznych dostawców usług ICT oraz liczba i rodzaj umów z zewnętrznymi dostawcami usług ICT lub dostawcami usług ICT wewnątrz grupy;

(vi) wyniki wszelkich przeglądów nadzorczych istotnych dla oceny zaawansowania podmiotu finansowego pod względem ICT;

(vii) dojrzałość planów ciągłości działania w zakresie ICT oraz planów reagowania i przywracania sprawności ICT;

(viii) dojrzałość operacyjnych środków wykrywania i ograniczania zagrożeń bezpieczeństwa ICT, w tym zdolność do:

1) stałego monitorowania infrastruktury ICT podmiotu finansowego;

2) wykrywania zdarzeń związanych z ICT w czasie rzeczywistym;

3) analizowania zdarzeń, o których mowa w ppkt 2;

4) reagowania na zdarzenia, o których mowa w ppkt 2, w sposób szybki i skuteczny;

(ix) to, czy podmiot finansowy należy do grupy działającej w sektorze finansowym na szczeblu unijnym lub krajowym i czy współdzieli z tą grupą systemy ICT.

Do celów lit. a) pkt (i) organ ds. TLPT w miarę możliwości bierze pod uwagę:

a) udział w rynku podmiotu finansowego na poziomie unijnym i krajowym;

b) zakres działań oferowanych przez podmiot finansowy;

c) udział w rynku usług świadczonych przez podmiot finansowy lub działań podejmowanych na szczeblu unijnym i krajowym.

Do celów lit. a) pkt (v) organ ds. TLPT w miarę możliwości bierze pod uwagę:

a) czy podmiot finansowy stosuje więcej niż jeden model biznesowy;

b) wzajemne powiązania różnych procesów biznesowych i powiązanych usług.

2. Organy ds. TLPT wymagają, aby wszystkie wymienione poniżej podmioty finansowe przeprowadziły TLPT, chyba że ocena, o której mowa w ust. 1, wskazuje w odniesieniu do danego podmiotu finansowego, że jego wpływ, kwestie stabilności finansowej dotyczące tego podmiotu finansowego lub jego profil ryzyka związanego z ICT nie uzasadniają przeprowadzenia TLPT:

a) instytucje kredytowe, które spełniają którykolwiek z poniższych warunków:

(i) zostały określone jako globalne instytucje o znaczeniu systemowym zgodnie z art. 131 dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE ([7]);

(ii) zostały określone jako inne instytucje o znaczeniu systemowym zgodnie z art. 131 dyrektywy 2013/36/UE;

(iii) są częścią globalnych instytucji o znaczeniu systemowym lub innych instytucji o znaczeniu systemowym;

([7]) 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) instytucje płatnicze, w przypadku których w każdym z dwóch lat kalendarzowych poprzedzających ocenę dokonaną przez organ ds. TLPT łączna wartość transakcji płatniczych zdefiniowanych w art. 4 pkt 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 przekroczyła 150 mld EUR ([8]);

c) instytucje pieniądza elektronicznego, w przypadku których w każdym z dwóch lat kalendarzowych poprzedzających ocenę dokonaną przez organ ds. TLPT łączna wartość transakcji płatniczych zdefiniowanych w art. 4 pkt 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 przekroczyła 150 mld EUR albo łączna wartość pieniądza elektronicznego pozostającego w obiegu przekroczyła 40 mld EUR;

d) centralne depozyty papierów wartościowych;

e) kontrahenci centralni;

f) systemy obrotu z elektronicznym systemem obrotu, które spełniają którekolwiek z poniższych kryteriów:

(i) system obrotu ma najwyższy udział w rynku pod względem obrotu na poziomie krajowym w każdym z dwóch lat kalendarzowych poprzedzających ocenę dokonaną przez organ ds. TLPT w którymkolwiek z obszarów, do których należą:

1) zbywalne papiery wartościowe zdefiniowane w art. 4 ust. 1 pkt 44 lit. a) dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE ([9]);

2) zbywalne papiery wartościowe zdefiniowane w art. 4 ust. 1 pkt 44 lit. b) dyrektywy 2014/65/UE;

3) instrumenty pochodne zdefiniowane w art. 2 ust. 1 pkt 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 600/2014 ([10]);

4) strukturyzowane produkty finansowe zdefiniowane w art. 2 ust. 1 pkt 28 rozporządzenia (UE) nr 600/2014;

5) uprawnienia do emisji, o których mowa w sekcji C pkt 11 załącznika I do dyrektywy 2014/65/UE;

(ii) w każdym z dwóch lat kalendarzowych poprzedzających ocenę dokonaną przez organ ds. TLPT udział systemu obrotu w rynku pod względem obrotu na poziomie Unii przekracza 5 % w którymkolwiek z poniższych obszarów, do których należą:

1) akcje spółek oraz inne papiery wartościowe odpowiadające akcjom spółek, udziałom w spółkach osobowych lub w innych podmiotach oraz kwity depozytowe dotyczące akcji lub udziałów;

2) obligacje lub innego rodzaju papiery dłużne, w tym kwity depozytowe dotyczące takich papierów wartościowych;

3) instrumenty pochodne zdefiniowane w art. 2 ust. 1 pkt 29 rozporządzenia (UE) nr 600/2014;

4) strukturyzowane produkty finansowe zdefiniowane w art. 2 ust. 1 pkt 28 rozporządzenia (UE) nr 600/2014;

5) uprawnienia do emisji, o których mowa w sekcji C pkt 11 załącznika I do dyrektywy 2014/65/UE;

([8]) 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).

([9]) 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, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) zakłady ubezpieczeń i zakłady reasekuracji, które spełniają wszystkie następujące kryteria:

(i) wysokość ich składki przypisanej brutto przekracza 1 500 000 000 EUR;

(ii) zakłady te posiadają rezerwy techniczno-ubezpieczeniowe przekraczające 10 000 000 000 EUR;

(iii) w przypadku zakładów ubezpieczeń, które prowadzą wyłącznie działalność w zakresie ubezpieczeń na życie lub które prowadzą zarówno działalność w zakresie ubezpieczeń na życie, jak i działalność w zakresie ubezpieczeń innych niż ubezpieczenia na życie – łączna wartość ich aktywów, wycenionych zgodnie z art. 75 dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE ([11]), przekracza 3,5 % łącznej wartości aktywów zakładów ubezpieczeń i zakładów reasekuracji mających siedzibę w danym państwie członkowskim.

Do celów lit. f) pkt (ii), w przypadku gdy system obrotu jest częścią grupy korzystającej ze wspólnych systemów ICT lub z tego samego dostawcy usług ICT wewnątrz grupy, uwzględnia się obrót z tytułu papierów wartościowych i kontraktów na instrumenty pochodne we wszystkich systemach obrotu należących do tej samej grupy i mających siedzibę w Unii.

Do celów lit. g) organy ds. TLPT określają podzbiór wszystkich zakładów ubezpieczeń i zakładów reasekuracji, stosując kryteria określone w lit. g) pkt (i), (ii) oraz (iii). Zakłady ubezpieczeń i zakłady reasekuracji należące do tego podzbioru są zobowiązane do przeprowadzenia TLPT, jeżeli spełniają również którekolwiek z następujących kryteriów:

a) wysokość ich składki przypisanej brutto przekracza 3 000 000 000 EUR;

b) ich rezerwy techniczno-ubezpieczeniowe przekraczają 30 000 000 000 EUR;

c) łączna wartość ich aktywów, wycenionych zgodnie z art. 75 dyrektywy 2009/138/WE, przekracza 10 % łącznej wartości aktywów zakładów ubezpieczeń i zakładów reasekuracji mających siedzibę w danym państwie członkowskim.

3. W przypadku gdy kryteria określone w ust. 2 spełnia więcej niż jeden podmiot finansowy należący do tej samej grupy i korzystający ze wspólnych systemów ICT lub więcej niż jeden podmiot finansowy korzystający z tego samego dostawcy usług ICT wewnątrz grupy, organy ds. TLPT tych podmiotów finansowych, zgodnie z art. 16 ust. 2, podejmują decyzję, czy do tych podmiotów finansowych ma zastosowanie wymóg indywidualnego przeprowadzania TLPT.

W przypadku gdy organ ds. TLPT właściwy dla jednostki dominującej grupy podmiotów finansowych, o której mowa w akapicie pierwszym, jest inny niż organy ds. TLPT właściwe dla podmiotów finansowych należących do tej grupy, organy ds. TLPT właściwe dla podmiotów finansowych należących do grupy konsultują się z organem właściwym dla jednostki dominującej w sprawie w zasadności indywidualnego przeprowadzania TLPT.

Artykuł 3

Zespół TCT i kierownicy testów na potrzeby TLPT

1. Organ ds. TLPT powierza odpowiedzialność za koordynację działań związanych z TLPT zespołowi TCT. Zespół TCT składa się z kierowników testów wyznaczonych do nadzorowania pojedynczego procesu TLPT.

2. Na potrzeby każdego testu organ ds. TLPT wyznacza kierownika testu i co najmniej jednego zastępcę.

3. Kierownicy testów monitorują, czy spełnione są wymogi określone w niniejszym rozporządzeniu, i zapewniają ich spełnienie.

([11]) 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, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Kierownik testu przekazuje podmiotowi finansowemu dane kontaktowe zespołu TCT w powiadomieniu, o którym mowa w art. 9 ust. 1.

5. Organ ds. TLPT uczestniczy we wszystkich etapach TLPT.

Artykuł 4

Rozwiązania organizacyjne dla podmiotów finansowych

1. Podmioty finansowe wyznaczają lidera zespołu typu control team, który odpowiada za bieżące zarządzanie TLPT oraz za decyzje i działania zespołu typu control team.

2. Podmioty finansowe ustanawiają środki organizacyjne i proceduralne w celu zapewnienia, aby:

a) dostęp do informacji dotyczących wszelkich planowanych lub trwających TLPT był ograniczony na zasadzie wiedzy koniecznej do zespołu typu control team, organu zarządzającego, testerów, dostawcy analizy zagrożeń i organu ds. TLPT;

b) przed zaangażowaniem jakiegokolwiek członka zespołu typu blue team w TLPT zespół typu control team konsultował się z kierownikami testów;

c) zespół typu control team był informowany o każdym wykryciu TLPT przez pracowników podmiotu finansowego lub jego zewnętrznych dostawców usług; w przypadku eskalacji reagowania na wynikłe incydenty, w razie potrzeby, zespół typu control team powstrzymał taką eskalację;

d) wprowadzono ustalenia dotyczące poufności TLPT, mające zastosowanie do pracowników podmiotu finansowego, pracowników zainteresowanych zewnętrznych dostawców usług ICT, testerów i dostawcy analizy zagrożeń;

e) zespół typu control team przekazywał kierownikom testów na ich wniosek wszelkie informacje dotyczące TLPT;

f) w miarę możliwości strony zaangażowane w TLPT nawiązywały do testów wyłącznie za pomocą kryptonimu.

Artykuł 5

Zarządzanie ryzykiem związanym z TLPT

1. Na etapie przygotowawczym, o którym mowa w art. 9, zespół typu control team ocenia ryzyko związane z testowaniem działających na bieżąco systemów produkcji wspierających krytyczne lub istotne funkcje podmiotu finansowego, w tym potencjalny wpływ testowania na:

a) sektor finansowy;

b) stabilność finansową na poziomie unijnym lub krajowym.

Zespół typu control team dokonuje przeglądu wspomnianego wpływu przez cały czas trwania testów.

2. Na potrzeby oceny ryzyka i zarządzania ryzykiem zespół typu control team uwzględnia co najmniej następujące rodzaje ryzyka:

a) ryzyko związane z udzieleniem dostępu, w stosownych przypadkach, dostawcy analizy zagrożeń i testerom zewnętrznym do szczególnie chronionych informacji na temat podmiotu finansowego;

b) ryzyko związane z brakiem zgodności TLPT z rozporządzeniem (UE) 2022/2554 i z niniejszym rozporządzeniem, jeżeli taki brak zgodności skutkuje brakiem poświadczenia, o którym mowa w art. 26 ust. 7 rozporządzenia (UE) 2022/2554, w tym w przypadku gdy taki brak zgodności wynika z naruszenia poufności TLPT lub z nieetycznego postępowania;

c) ryzyko związane z eskalacją sytuacji kryzysowych i incydentów;

d) ryzyko związane z etapem aktywnego testowania z udziałem zespołu typu red team, w tym ryzyko związane z przerwaniem krytycznej działalności i uszkodzeniem danych w wyniku działań testerów, oraz jego potencjalny wpływ na osoby trzecie;

e) ryzyko związane z działaniami zespołu typu blue team, w tym ryzyko związane z przerwaniem krytycznej działalności i uszkodzeniem danych w wyniku działań zespołu typu blue team, oraz jego potencjalny wpływ na osoby trzecie;

f) ryzyko związane z niepełnym przywróceniem sprawności systemów objętych TLPT.

Artykuł 6

Zarządzanie ryzykiem w przypadku zbiorczych lub wspólnych TLPT

1. W przypadku wspólnych TLPT lub zbiorczych TLPT zespół typu control team każdego podmiotu finansowego przeprowadza własną ocenę ryzyka i ustanawia własne środki zarządzania ryzykiem.

2. Zespół typu control team wyznaczonego podmiotu finansowego, o którym mowa w art. 16 ust. 3 lit. b) niniejszego rozporządzenia, lub podmiot finansowy wyznaczony zgodnie z art. 26 ust. 4 rozporządzenia (UE) 2022/2554 oceniają ryzyko związane z udziałem w TLPT wielu podmiotów finansowych. Zespoły typu control team zaangażowanych podmiotów finansowych współpracują z zespołem typu control team wyznaczonego podmiotu finansowego w celu określenia potencjalnego wspólnego ryzyka.

Artykuł 7

Wybór dostawców TLPT

1. Zespół typu control team wprowadza środki zarządzania ryzykiem związanym z TLPT, a w szczególności zapewnia, by w przypadku każdego TLPT:

a) dostawca analizy zagrożeń i zewnętrzni testerzy dostarczyli zespołowi typu control team szczegółowy życiorys i kopie certyfikatów, które zgodnie z uznanymi standardami rynkowymi stanowią poświadczenie ich odpowiedniości do wykonywania powierzonych im zadań;

b) dostawca analizy zagrożeń i zewnętrzni testerzy byli należycie i w pełni objęci odpowiednimi ubezpieczeniami od odpowiedzialności cywilnej z tytułu wykonywania zawodu, w tym od ryzyka uchybień i zaniedbań;

c) dostawca analizy zagrożeń przedstawił co najmniej trzy rekomendacje z powierzonych mu poprzednio zadań w zakresie testów penetracyjnych i testów z udziałem zespołu typu red team;

d) testerzy zewnętrzni przedstawili co najmniej pięć rekomendacji z powierzonych im poprzednio zadań w zakresie testów penetracyjnych i testów z udziałem zespołu typu red team;

e) personel dostawcy analizy zagrożeń przydzielony do TLPT:

(i) obejmował co najmniej kierownika z co najmniej pięcioletnim doświadczeniem w zakresie analizy zagrożeń oraz co najmniej jednego dodatkowego członka z co najmniej dwuletnim doświadczeniem w zakresie analizy zagrożeń;

(ii) wykazywał się szerokim zakresem i odpowiednim poziomem wiedzy i umiejętności zawodowych, obejmujących:

1) taktyki, techniki i procedury gromadzenia danych wywiadowczych;

2) wiedzę geopolityczną, techniczną i sektorową;

3) odpowiednie umiejętności komunikacyjne umożliwiające jasne przedstawianie wyników jego pracy i składanie sprawozdań na ten temat;

(iii) brał łącznie udział w co najmniej trzech wcześniejszych zadaniach związanych z analizą zagrożeń w kontekście testów penetracyjnych i testów z udziałem zespołu typu red team;

(iv) nie wykonywał jednocześnie żadnych zadań zespołu typu blue team ani innych usług, które mogą stanowić konflikt interesów w odniesieniu do podmiotu finansowego, zewnętrznego dostawcy usług ICT lub dostawcy usług ICT wewnątrz grupy zaangażowanych w TLPT, do których personel ten został przydzielony;

(v) był oddzielony od personelu tego samego dostawcy TLPT, który zapewnia testerów zewnętrznych na potrzeby tych samych TLPT, i nie podlegał temu personelowi;

f) w przypadku testerów zewnętrznych zespół typu red team przydzielony do TLPT:

(i) składał się co najmniej z kierownika posiadającego co najmniej pięcioletnie doświadczenie w testach penetracyjnych i testach z udziałem zespołu typu red team, a także z co najmniej dwóch dodatkowych testerów, z których każdy posiada co najmniej dwuletnie doświadczenie w testach penetracyjnych i testach z udziałem zespołu typu red team;

(ii) wykazywał się szerokim zakresem i odpowiednim poziomem wiedzy i umiejętności zawodowych, obejmujących wiedzę na temat działalności podmiotu finansowego, rozpoznania, zarządzania ryzykiem, opracowywania exploitów, penetracji fizycznej, inżynierii społecznej, analizy podatności na zagrożenia, a także odpowiednimi umiejętnościami komunikacyjnymi umożliwiającymi jasne przedstawienie wyników jego pracy i składanie sprawozdań na ten temat;

(iii) brał łącznie udział w co najmniej pięciu wcześniejszych zadaniach związanych z testami penetracyjnymi i testami z udziałem zespołu typu red team;

(iv) nie był zatrudniony przez dostawcę analizy zagrożeń, który jednocześnie wykonuje zadania zespołu typu blue team na rzecz podmiotu finansowego, zewnętrznego dostawcy usług ICT lub dostawcy usług ICT wewnątrz grupy zaangażowanych w TLPT, ani nie świadczył usług na rzecz takiego dostawcy analizy zagrożeń;

(v) był oddzielony od personelu tego samego dostawcy TLPT, który jednocześnie świadczy usługi w zakresie analizy zagrożeń na potrzeby tych samych TLPT;

g) po zakończeniu testów testerzy i dostawca analizy zagrożeń realizowali procedury przywracania danych, obejmujące bezpieczne usuwanie informacji związanych z hasłami, danymi uwierzytelniającymi i innymi tajnymi kluczami, których bezpieczeństwo zostało naruszone podczas TLPT, bezpieczną komunikację z podmiotami finansowymi, których konta zostały naruszone, bezpieczne gromadzenie, przechowywanie i usuwanie innych danych zebranych podczas testów oraz zarządzanie nimi;

h) testerzy, oprócz procedur przywracania danych po zakończeniu testowania, o których mowa w lit. g), realizowali następujące procedury przywracania:

(i) dezaktywacja dowodzenia i kierowania;

(ii) aktywacja wyłączników awaryjnych w przypadku przekroczenia zakresu i daty;

(iii) usuwanie backdoorów i innego złośliwego oprogramowania;

(iv) powiadamianie o potencjalnych naruszeniach;

(v) procedury umożliwiające przywrócenie kopii zapasowej w przyszłości, co może być konieczne z uwagi na złośliwe oprogramowanie lub narzędzia zainstalowane podczas testu;

(vi) monitorowanie działań zespołu typu blue team i informowanie zespołu typu control team o wszelkich możliwych przypadkach wykrycia;

i) testerzy i dostawca analizy zagrożeń nie wykonywali żadnego z następujących działań ani nie uczestniczyli w takich działaniach:

(i) nieuprawnione zniszczenie sprzętu podmiotu finansowego i jego zewnętrznych dostawców usług ICT, jeśli tacy istnieją;

(ii) niekontrolowana modyfikacja informacji i zasobów ICT podmiotu finansowego i jego zewnętrznych dostawców usług ICT, jeśli tacy istnieją;

(iii) celowe naruszenie ciągłości krytycznych lub istotnych funkcji podmiotu finansowego;

(iv) nieuprawnione włączenie do testów systemów nieobjętych ich zakresem;

(v) nieuprawnione ujawnienie wyników testów.

2. W celu wykazania zgodności z ust. 1 lit. a)–f) zespół typu control team ewidencjonuje dokumentację dostarczoną przez testerów i dostawców analizy zagrożeń.

W wyjątkowych okolicznościach podmioty finansowe mogą zawierać umowy z zewnętrznymi testerami i dostawcami analizy zagrożeń, którzy nie spełniają jednego lub większej liczby wymogów określonych w ust. 1 lit. a)–f), pod warunkiem że te podmioty finansowe przyjmą odpowiednie środki służące ograniczeniu ryzyka związanego z brakiem zgodności z wspomnianymi literami i udokumentują te środki.

Artykuł 8

Szczególne postanowienia dotyczące zbiorczych lub wspólnych TLPT

1. O ile wiodący organ ds. TLPT nie postanowi inaczej, w przypadku gdy kilka podmiotów finansowych określonych zgodnie z art. 16 ust. 2 lub 4 bierze udział w zbiorczych lub wspólnych TLPT, każdy podmiot finansowy realizuje każdy z etapów określonych w art. 9–15.

2. O ile niniejsze rozporządzenie nie stanowi inaczej, w przypadku gdy we wspólne TLPT lub w zbiorcze TLPT, o których mowa w art. 16 ust. 3 lub art. 16 ust. 5, zaangażowanych jest kilka organów ds. TLPT, odniesienia w art. 9–15 do „organu ds. TLPT" należy rozumieć jako odniesienia do wiodącego organu ds. TLPT właściwego dla takich zbiorczych lub wspólnych TLPT.

Artykuł 9

Etap przygotowawczy

1. Podmiot finansowy określony zgodnie z art. 26 ust. 8 akapit trzeci rozporządzenia (UE) 2022/2554 inicjuje TLPT po otrzymaniu od organu ds. TLPT powiadomienia o konieczności przeprowadzenia TLPT.

2. W terminie 3 miesięcy od otrzymania powiadomienia, o którym mowa w ust. 1, podmiot finansowy przekazuje kierownikom testów wszystkie następujące informacje związane z inicjacją TLPT:

a) kartę projektu zawierającą wysokopoziomowy plan projektu, obejmujący informacje określone w załączniku I;

b) dane kontaktowe lidera zespołu typu control team;

c) informację, czy planowane jest wykorzystanie testerów wewnętrznych czy zewnętrznych, czy też, w stosownych przypadkach, jednych i drugich, jak określono w art. 15;

d) informacje na temat kanałów komunikacji, które będą wykorzystywane podczas TLPT;

e) kryptonim TLPT.

3. Jeżeli informacje, o których mowa w ust. 2 lit. a)–e), są kompletne oraz zapewniają odpowiedniość i skuteczność TLPT, organ ds. TLPT zatwierdza przedłożone przez podmiot finansowy informacje związane z inicjacją TLPT i powiadamia o tym podmiot finansowy.

4. Po zatwierdzeniu przez organ ds. TLPT informacji o inicjacji TLPT podmiot finansowy powołuje zespół typu control team, który wspiera lidera zespołu typu control team w wykonywaniu następujących zadań:

a) określenie kanałów i procesów komunikacji w obrębie zespołu typu control team oraz z testerami i dostawcami analizy zagrożeń we wszystkich kwestiach związanych z TLPT;

b) informowanie organu zarządzającego podmiotu finansowego o postępach w TLPT i o związanym z nimi ryzyku;

c) podejmowanie decyzji w oparciu o merytoryczną wiedzę specjalistyczną przez cały czas trwania TLPT;

d) przeprowadzanie TLPT zgodnie z niniejszym rozporządzeniem;

e) wybór dostawcy analizy zagrożeń na potrzeby TLPT;

f) wybór testerów zewnętrznych, testerów wewnętrznych lub obu rodzajów testerów;

g) przygotowanie dokumentu określającego zakres.

5. Jeżeli organ ds. TLPT uzna, że początkowy skład zespołu typu control team i wszelkie późniejsze zmiany w tym składzie umożliwiają odpowiednie wykonywanie zadań, o których mowa w ust. 4, organ ds. TLPT zatwierdza zespół typu control team i powiadamia o tym lidera tego zespołu.

6. W terminie 6 miesięcy od otrzymania powiadomienia od organu ds. TLPT, o którym to powiadomieniu mowa w ust. 1, podmiot finansowy przekazuje kierownikom testów dokument określający zakres zawierający wszystkie informacje wskazane w załączniku II. Organ zarządzający podmiotu finansowego zatwierdza dokument określający zakres.

7. Podmioty finansowe podejmują decyzję o objęciu zakresem TLPT krytycznych lub istotnych funkcji, biorąc pod uwagę następujące kryteria:

a) krytyczny lub istotny charakter danej funkcji oraz jej ewentualny wpływ na sektor finansowy i stabilność finansową na szczeblu unijnym i krajowym;

b) znaczenie funkcji dla bieżącej działalności gospodarczej podmiotu finansowego;

c) wymienność funkcji;

d) wzajemne powiązania z innymi funkcjami;

e) położenie geograficzne funkcji;

f) sektorową zależność innych podmiotów od funkcji;

g) w miarę dostępności – analizę zagrożeń dotyczącą tej funkcji.

8. Po zawarciu umowy z testerami i dostawcami analizy zagrożeń zespół typu control team udostępnia im informacje związane z inicjacją TLPT oraz dokument określający zakres. Zespół typu control team informuje testerów i dostawców analizy zagrożeń o procesie testowania, który będzie realizowany.

9. Podmiot finansowy dopilnowuje, aby pozyskiwanie lub wyznaczanie testerów i dostawców analizy zagrożeń zostało zakończone przed rozpoczęciem etapu testowania.

10. Przed rozpoczęciem etapu testowania zespół typu control team konsultuje się z kierownikami testów w sprawie oceny ryzyka związanego z TLPT i środków zarządzania ryzykiem. Zespół typu control team dokonuje przeglądu oceny ryzyka lub środków zarządzania ryzykiem, jeżeli organ ds. TLPT jest zdania, że nie uwzględniają one w odpowiedni sposób ryzyka związanego z TLPT.

11. Zespół typu control team ocenia, czy dostawcy analizy zagrożeń i testerzy, których bierze pod uwagę pod kątem udziału w TLPT, spełniają wymogi określone w art. 27 rozporządzenia (UE) 2022/2554 i art. 7 ust. 1 niniejszego rozporządzenia, oraz dokumentuje wynik tej oceny. Zespół typu control team wybiera dostawców analizy zagrożeń zgodnie z tą oceną i swoimi praktykami zarządzania ryzykiem. Przed zawarciem umowy z wybranymi dostawcami analizy zagrożeń i zewnętrznymi testerami zespół typu control team przedstawia kierownikom testów dowody potwierdzające spełnianie przez tych dostawców analizy zagrożeń i testerów wymogów określonych w art. 27 rozporządzenia (UE) 2022/2554 oraz w art. 7 ust. 1 niniejszego rozporządzenia. Zespół typu control team nie może zawrzeć umowy z wybranymi dostawcami analizy zagrożeń i testerami zewnętrznymi, jeżeli organ ds. TLPT jest zdania, że ci wybrani dostawcy analizy zagrożeń i testerzy zewnętrzni nie spełniają wymogów określonych w art. 27 rozporządzenia (UE) 2022/2554 lub wymogów określonych w art. 7 ust. 1 niniejszego rozporządzenia, lub dodatkowych wymogów wynikających z krajowych przepisów dotyczących bezpieczeństwa zgodnie z prawem Unii, lub jeżeli podmiot finansowy nie spełnia wymogów określonych w art. 7 ust. 2 akapit pierwszy niniejszego rozporządzenia lub jeżeli nie są spełnione warunki, o których mowa w art. 7 ust. 2 akapit drugi niniejszego rozporządzenia.

12. Jeżeli dokument określający zakres jest kompletny i zapewnia odpowiednie przeprowadzenie skutecznych TLPT, organ ds. TLPT zatwierdza ten dokument i informuje o tym lidera zespołu typu control team.

Artykuł 10

Etap testowania: analiza zagrożeń

1. Po zatwierdzeniu przez organ ds. TLPT dokumentu określającego zakres dostawca analizy zagrożeń bada analizę zagrożeń ogólnych i sektorowych istotnych dla podmiotu finansowego. W przypadku gdy organ ds. TLPT stworzył ogólny krajobraz zagrożeń dla sektora finansowego państwa członkowskiego, dostawca analizy zagrożeń może wykorzystać ten krajobraz jako punkt odniesienia dla krajowego krajobrazu zagrożeń. Dostawca analizy zagrożeń identyfikuje cyberzagrożenia oraz istniejące lub potencjalne podatności dotyczące danego podmiotu finansowego. Ponadto dostawca analizy zagrożeń gromadzi i analizuje konkretne, użyteczne i kontekstowe dane wywiadowcze dotyczące celów i zagrożeń w odniesieniu do podmiotu finansowego, w tym za pośrednictwem konsultacji z zespołem typu control team i kierownikami testów.

2. Dostawca analizy zagrożeń dokonuje prezentacji odnośnych zagrożeń i ukierunkowanej analizy zagrożeń oraz proponuje wymagane scenariusze zespołowi typu control team, testerom i kierownikom testów. Proponowane scenariusze muszą różnić się pod względem zidentyfikowanych agresorów i powiązanych taktyk, technik i procedur oraz muszą być ukierunkowane na każdą krytyczną lub istotną funkcję objętą zakresem TLPT.

3. Lider zespołu typu control team wybiera co najmniej trzy scenariusze przeprowadzenia TLPT, biorąc pod uwagę wszystkie następujące elementy:

a) zalecenie dostawcy analizy zagrożeń i potencjał każdego scenariusza w zakresie wyszukiwania zagrożeń;

b) informacje przekazane przez kierowników testów;

c) wykonalność scenariuszy proponowanych do realizacji, w oparciu o ocenę ekspercką testerów;

d) wielkość, złożoność i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i złożoność jego usług, działalności i operacji.

4. Nie więcej niż jeden z wybranych scenariuszy może nie być związany z wyszukiwaniem istniejących zagrożeń i może opierać się na potencjalnie fikcyjnym przyszłym zagrożeniu o wysokiej wartości predykcyjnej, antycypacyjnej, oportunistycznej lub prospektywnej, biorąc pod uwagę przewidywany rozwój krajobrazu zagrożeń dotyczącego podmiotu finansowego.

W przypadku zbiorczych TLPT, bez uszczerbku dla scenariuszy ukierunkowanych bezpośrednio na krytyczne lub istotne funkcje podmiotów finansowych uczestniczących w testowaniu, co najmniej jeden scenariusz musi obejmować istotne systemy, procesy i technologie ICT zewnętrznego dostawcy usług ICT wspierające krytyczne lub istotne funkcje podmiotów finansowych objętych badaniem.

W przypadku wspólnych TLPT obejmujących dostawcę usług ICT wewnątrz grupy, bez uszczerbku dla scenariuszy ukierunkowanych bezpośrednio na krytyczne lub istotne funkcje podmiotów finansowych uczestniczących w testowaniu, co najmniej jeden scenariusz musi obejmować istotne systemy, procesy i technologie ICT dostawcy usług ICT wewnątrz grupy wspierające krytyczne lub istotne funkcje podmiotów finansowych objętych badaniem.

5. Dostawca analizy zagrożeń przekazuje zespołowi typu control team sprawozdanie z ukierunkowanej analizy zagrożeń, w tym scenariusze wybrane zgodnie z ust. 3 i 4. Sprawozdanie z analizy zagrożeń zawiera informacje określone w załączniku III.

6. Zespół typu control team przedkłada kierownikowi testu do zatwierdzenia sprawozdanie z ukierunkowanej analizy zagrożeń. Jeżeli sprawozdanie z ukierunkowanej analizy zagrożeń jest kompletne i zapewnia przeprowadzenie skutecznych TLPT, organ ds. TLPT zatwierdza ten dokument i informuje o tym lidera zespołu typu control team.

Artykuł 11

Etap testowania: testy z udziałem zespołu typu red team

1. Po zatwierdzeniu przez organ ds. TLPT sprawozdania z ukierunkowanej analizy zagrożeń testerzy przygotowują plan testów z udziałem zespołu typu red team, który to plan zawiera informacje określone w załączniku IV. Jako podstawę do tworzenia scenariuszy ataków testerzy wykorzystują dokument określający zakres i sprawozdanie z ukierunkowanej analizy zagrożeń.

2. Testerzy konsultują się z zespołem typu control team, dostawcą analizy zagrożeń i kierownikami testów w sprawie planu testów z udziałem zespołu typu red team, w tym ustaleń dotyczących komunikacji, procedur i zarządzania projektem, przygotowania i przypadków użycia ułatwień oraz ustaleń dotyczących składania sprawozdań zespołowi typu control team i kierownikom testów.

3. Jeżeli plan testów z udziałem zespołu typu red team jest kompletny i zapewnia przeprowadzenie skutecznych TLPT, zespół typu control team i organ ds. TLPT zatwierdza ten plan i informuje o tym lidera zespołu typu control team.

4. Po zatwierdzeniu planu testów z udziałem zespołu typu red team zgodnie z ust. 3 testerzy przeprowadzają TLPT podczas etapu aktywnego testowania z udziałem zespołu typu red team.

5. Czas trwania etapu aktywnego testowania z udziałem zespołu typu red team jest proporcjonalny do zakresu TLPT, skali, działalności, złożoności i liczby podmiotów finansowych oraz zewnętrznych dostawców usług ICT lub dostawców usług ICT wewnątrz grupy zaangażowanych w TLPT, a w każdym przypadku trwa co najmniej 12 tygodni. Scenariusze ataku można realizować kolejno lub jednocześnie. Zespół typu control team, dostawca analizy zagrożeń, testerzy i kierownicy testów uzgadniają zakończenie fazy aktywnego testowania z udziałem zespołu typu red team.

6. Pod warunkiem zapewnienia, by plan testów z udziałem zespołu typu red team pozostał kompletny i umożliwiał przeprowadzenie skutecznych testów TLPT, lider zespołu typu control team i kierownicy testów zatwierdzają wszelkie zmiany w planie testów z udziałem zespołu typu red team wprowadzone po jego zatwierdzeniu, w tym zmiany dotyczące harmonogramu, zakresu, wybranych systemów lub flag.

7. Podczas całego etapu aktywnego testowania z udziałem zespołu typu red team testerzy co najmniej raz w tygodniu składają zespołowi typu control team i kierownikom testów sprawozdania z postępów w TLPT, a dostawca analizy zagrożeń pozostaje dostępny w razie potrzeby konsultacji i przeprowadzenia dodatkowej analizy zagrożeń na wniosek zespołu typu control team.

8. Zespół typu control team dostarcza w odpowiednim czasie ułatwienia zaprojektowane na podstawie planu testów z udziałem zespołu typu red team. Za zgodą zespołu typu control team i kierowników testów można dodawać kolejne ułatwienia lub je dostosowywać.

9. W przypadku wykrycia testowania przez któregoś członka personelu podmiotu finansowego lub, w stosownych przypadkach, jego zewnętrznych dostawców usług ICT lub dostawcy usług ICT wewnątrz grupy zespół typu control team, w porozumieniu z testerami i bez uszczerbku dla ust. 10, proponuje i przedkłada kierownikom testów do zatwierdzenia środki umożliwiające kontynuowanie TLPT przy jednoczesnym zapewnieniu poufności tego procesu.

10. W wyjątkowych okolicznościach stwarzających ryzyko wpływu na dane, szkód dla zasobów i zakłócenia krytycznych lub istotnych funkcji, usług lub operacji samego podmiotu finansowego, jego zewnętrznych dostawców usług ICT lub dostawców usług ICT wewnątrz grupy bądź zakłóceń dla jego kontrahentów lub sektora finansowego, lider zespołu typu control team może zawiesić TLPT lub, w ostateczności, w przypadku gdy kontynuacja TLPT nie jest możliwa w inny sposób i z zastrzeżeniem uprzedniego zatwierdzenia przez organ ds. TLPT, kontynuować TLPT, realizując ograniczone działania z udziałem zespołu typu purple team. Czas trwania ograniczonych działań z udziałem zespołu typu purple team wlicza się do minimalnego 12-tygodniowego czasu trwania etapu aktywnego testowania z udziałem zespołu typu red team, o którym mowa w ust. 5.

Artykuł 12

Etap zamykania

1. Po zakończeniu etapu aktywnego testowania z udziałem zespołu typu red team lider zespołu typu control team informuje zespół typu blue team o tym, że przeprowadzono TLPT.

2. W ciągu czterech tygodni od zakończenia etapu aktywnego testowania z udziałem zespołu typu red team testerzy przedkładają zespołowi typu control team sprawozdanie z testów sporządzone przez zespół typu red team, zawierające informacje określone w załączniku V.

3. Zespół typu control team bez zbędnej zwłoki przekazuje zespołowi typu blue team i kierownikom testów sprawozdanie z testów sporządzone przez zespół typu red team.

Na wniosek kierowników testów sprawozdanie, o którym mowa w akapicie pierwszym, nie zawiera informacji szczególnie chronionych.

4. Po otrzymaniu sprawozdania z testów sporządzonego przez zespół typu red team i nie później niż 10 tygodni po zakończeniu etapu aktywnego testowania z udziałem zespołu typu red team zespół typu blue team przedkłada zespołowi typu control team sprawozdanie z testów sporządzone przez zespół typu blue team, zawierające informacje określone w załączniku VI. Zespół typu control team bez zbędnej zwłoki przekazuje testerom i kierownikom testów sprawozdanie z testów sporządzone przez zespół typu blue team.

Na wniosek kierowników testów sprawozdanie, o którym mowa w akapicie pierwszym, nie zawiera informacji szczególnie chronionych.

5. Nie później niż 10 tygodni po zakończeniu etapu aktywnego testowania z udziałem zespołu typu red team zespół typu blue team i testerzy odtwarzają działania ofensywne i obronne podejmowane podczas TLPT. Zespół typu control team przeprowadza również działanie z udziałem zespołu typu purple team w odniesieniu do tematów wspólnie wskazanych przez zespół typu blue team i testerów, dotyczące podatności zidentyfikowanych podczas testów oraz, w stosownych przypadkach, kwestii, których nie można było przetestować podczas etapu aktywnego testowania z udziałem zespołu typu red team.

6. Po zakończeniu odtwarzania działań podjętych podczas testów i zakończeniu działań z udziałem zespołu typu purple team zespół typu control team, zespół typu blue team, testerzy i dostawcy analizy zagrożeń przekazują sobie nawzajem informacje zwrotne na temat procesu TLPT. Informacje zwrotne mogą być również przekazywane przez kierowników testów.

7. Po powiadomieniu lidera zespołu typu control team przez organ ds. TLPT, że w jego ocenie sprawozdanie z testów sporządzone przez zespół typu blue team i sprawozdanie z testów sporządzone przez zespół typu red team zawierają informacje określone w załącznikach V i VI, w terminie 8 tygodni podmiot finansowy przedkłada do zatwierdzenia organowi ds. TLPT, o którym mowa w art. 26 ust. 6 rozporządzenia (UE) 2022/2554, sprawozdanie podsumowujące istotne ustalenia z TLPT, zawierające elementy określone w załączniku VII.

Na wniosek organu ds. TLPT sprawozdanie, o którym mowa w akapicie pierwszym, nie zawiera informacji szczególnie chronionych.

Artykuł 13

Plan naprawczy

1. W terminie 8 tygodni od powiadomienia, o którym mowa w art. 12 ust. 7 niniejszego rozporządzenia, podmiot finansowy przekazuje plany naprawcze i dokumentację, o której mowa w art. 26 ust. 6 rozporządzenia (UE) 2022/2554, organowi ds. TLPT oraz, jeżeli jest to inny organ, właściwemu organowi tego podmiotu finansowego.

2. Plan naprawczy, o którym mowa w ust. 1, obejmuje, w odniesieniu do każdego ustalenia dokonanego w ramach TLPT:

a) opis stwierdzonych niedociągnięć;

b) opis proponowanych środków naprawczych oraz ich hierarchii ważności i oczekiwanego zakończenia, w tym, w stosownych przypadkach, środków mających na celu poprawę zdolności identyfikacji, ochrony, wykrywania i reagowania;

c) analizę podstawowych przyczyn;

d) informacje na temat pracowników lub funkcji podmiotu finansowego odpowiedzialnych za wdrożenie proponowanych środków naprawczych lub ulepszeń;

e) ryzyko związane z niewdrożeniem środków, o których mowa w lit. b), oraz, w stosownych przypadkach, ryzyko związane z wdrażaniem takich środków.

Artykuł 14

Poświadczenie

1. Poświadczenie, o którym mowa w art. 26 ust. 7 rozporządzenia (UE) 2022/2554, zawiera informacje określone w załączniku VIII.

2. W przypadku gdy w TLPT było zaangażowanych kilka organów ds. TLPT, poświadczenie, o którym mowa w art. 26 ust. 7 rozporządzenia (UE) 2022/2554, jest przekazywane podmiotom finansowym poddanym testom przez wiodący organ ds. TLPT.

Artykuł 15

Korzystanie z testerów wewnętrznych

1. Podmioty finansowe ustanawiają wszystkie poniższe środki na potrzeby korzystania z testerów wewnętrznych:

a) ustanowienie i wdrożenie polityki zarządzania testerami wewnętrznymi podczas TLPT;

b) środki służące zapewnieniu, aby korzystanie z testerów wewnętrznych do przeprowadzania TLPT nie miało negatywnego wpływu na ogólne zdolności podmiotu finansowego w zakresie obrony lub odporności na incydenty związane z ICT ani nie miało znaczącego wpływu na dostępność zasobów przeznaczonych na zadania związane z ICT podczas TLPT;

c) środki służące zapewnieniu, aby testerzy wewnętrzni posiadali wystarczające zasoby i zdolności do przeprowadzenia TLPT.

Polityka, o której mowa w lit. a):

a) zawiera kryteria oceny odpowiedniości, kompetencji i potencjalnych konfliktów interesów testerów wewnętrznych oraz określa obowiązki zarządcze w procesie testowania;

b) jest dokumentowana i poddawana okresowym przeglądom;

c) zapewnia, aby w skład zespołu testerów wewnętrznych wchodził lider testów i co najmniej dwóch dodatkowych członków;

d) zawiera wymóg, aby wszyscy członkowie zespołu testerów byli zatrudnieni przez podmiot finansowy lub przez dostawcę usług ICT wewnątrz grupy przez ostatnie 12 miesięcy;

e) uwzględnia przepisy dotyczące szkolenia testerów wewnętrznych w zakresie sposobu przeprowadzania testów penetracyjnych i testów z udziałem zespołu typu red team.

2. Przy zatwierdzaniu przez organ ds. TLPT korzystania z testerów wewnętrznych zgodnie z art. 27 ust. 2 lit. a) rozporządzenia (UE) 2022/2554 organ ds. TLPT uwzględnia wymogi określone w art. 7 ust. 1 niniejszego rozporządzenia.

3. Korzystając z testerów wewnętrznych, podmiot finansowy zapewnia, aby takie korzystanie zostało wymienione w następujących dokumentach:

a) informacjach dotyczących inicjacji testów, o których mowa w art. 9;

b) sprawozdaniu z testów sporządzonym przez zespół typu red team, o którym to sprawozdaniu mowa w art. 12 ust. 2;

c) sprawozdaniu podsumowującym najbardziej istotne ustalenia z TLPT, o którym mowa w art. 26 ust. 6 rozporządzenia (UE) 2022/2554.

4. Testerów zatrudnionych przez dostawcę usług ICT wewnątrz grupy uznaje się za testerów wewnętrznych podmiotu finansowego.

Artykuł 16

Współpraca i wzajemne uznawanie

1. Do celów przeprowadzenia TLPT w odniesieniu do podmiotu finansowego świadczącego usługi w więcej niż jednym państwie członkowskim, w tym za pośrednictwem oddziału, jego organ ds. TLPT:

a) ustala, które organy ds. TLPT w przyjmujących państwach członkowskich należy zaangażować, biorąc pod uwagę, czy co najmniej jedna krytyczna lub istotna funkcja jest realizowana w przyjmujących państwach członkowskich lub jest współdzielona przez te państwa;

b) informuje organy ds. TLPT określone zgodnie z lit. a) o decyzji, by poddać podmiot finansowy testom TLPT;

c) o ile organy ds. TLPT nie uzgodnią inaczej, organ ds. TLPT właściwy dla podmiotu finansowego kieruje TLPT.

W ciągu 20 dni roboczych od otrzymania informacji o planowanym przeprowadzeniu TLPT organy ds. TLPT przyjmujących państw członkowskich mogą wyrazić zainteresowanie udziałem w TLPT w charakterze obserwatorów albo wyznaczyć kierownika testów do udziału w TLPT. Wiodący organ ds. TLPT przekazuje wszystkim organom ds. TLPT uczestniczącym w TLPT w charakterze obserwatorów dokument określający zakres, sprawozdanie podsumowujące z testów, plan naprawczy i poświadczenie.

Wiodący organ ds. TLPT koordynuje działania wszystkich uczestniczących organów ds. TLPT przez cały czas trwania testów i podejmuje wszelkie decyzje niezbędne do właściwego i skutecznego przeprowadzenia TLPT. Wiodący organ ds. TLPT może ustalić maksymalną liczbę uczestniczących organów ds. TLPT, jeżeli uczestnictwo większej ich liczby mogłoby zagrozić skutecznemu przeprowadzeniu TLPT.

2. W przypadku gdy podmiot finansowy korzysta z tego samego dostawcy usług ICT wewnątrz grupy co podmioty finansowe mające siedzibę w innych państwach członkowskich lub należy do grupy i współdzieli systemy ICT z podmiotami finansowymi z tej samej grupy mającymi siedzibę w innych państwach członkowskich, organ ds. TLPT podmiotu finansowego kontaktuje się z organami ds. TLPT innych podmiotów finansowych korzystających z tego samego dostawcy usług ICT wewnątrz grupy lub współdzielących systemy ICT w ramach grupy i ocenia wraz z nimi wykonalność i stosowność przeprowadzenia dla tych podmiotów wspólnych TLPT. Przeprowadzenie wspólnych TLPT uznaje się za lepsze rozwiązanie niż przeprowadzenie indywidualnych TLPT, jeżeli może to skutkować ograniczeniem kosztów i zasobów podmiotów finansowych i organów ds. TLPT, pod warunkiem że nie wpłynie to negatywnie na rzetelność i skuteczność testów.

3. Na potrzeby przeprowadzenia wspólnych TLPT:

a) organy ds. TLPT podmiotów finansowych uzgadniają, który podmiot finansowy zostanie wyznaczony do przeprowadzenia TLPT, biorąc pod uwagę strukturę grupy i skuteczność testu;

b) organ ds. TLPT podmiotu finansowego wyznaczonego zgodnie z lit. a) kieruje TLPT, chyba że organy ds. TLPT podmiotów finansowych uczestniczących we wspólnych TLPT uzgodnią inaczej;

c) organy ds. TLPT podmiotów finansowych innych niż podmiot finansowy wyznaczony do kierowania wspólnymi TLPT mogą wyrazić zainteresowanie śledzeniem TLPT w charakterze obserwatorów albo przydzielić kierownika testów do tych TLPT.

Wiodący organ ds. TLPT koordynuje działania wszystkich organów ds. TLPT zaangażowanych we wspólne TLPT i podejmuje wszystkie decyzje niezbędne do przeprowadzenia wspólnych TLPT w prawidłowy i skuteczny sposób.

4. W przypadku gdy podmiot finansowy zamierza przeprowadzić zbiorcze TLPT, o których mowa w art. 26 ust. 4 rozporządzenia (UE) 2022/2554, z ewentualnym udziałem podmiotów finansowych mających siedzibę w innych państwach członkowskich, jego organ ds. TLPT kontaktuje się z organami ds. TLPT pozostałych podmiotów finansowych i wraz z nimi ocenia wykonalność i stosowność przeprowadzenia dla tych podmiotów zbiorczych TLPT zgodnie z art. 26 ust. 4 rozporządzenia (UE) 2022/2554.

5. Na potrzeby przeprowadzenia zbiorczych TLPT, o których mowa w art. 26 ust. 4 rozporządzenia (UE) 2022/2554:

a) organy ds. TLPT podmiotów finansowych uzgadniają, który podmiot finansowy zostanie wyznaczony do prowadzenia zbiorczych TLPT, biorąc pod uwagę usługi ICT świadczone przez zewnętrznego dostawcę usług ICT na rzecz podmiotów finansowych oraz skuteczność testu;

b) organ ds. TLPT podmiotu finansowego wyznaczonego zgodnie z lit. a) kieruje TLPT, chyba że organy ds. TLPT podmiotów finansowych uczestniczących w zbiorczych TLPT uzgodnią inaczej;

c) organy ds. TLPT podmiotów finansowych innych niż podmiot finansowy wyznaczony do kierowania zbiorczymi TLPT mogą wyrazić zainteresowanie śledzeniem TLPT w charakterze obserwatorów albo przydzielić kierownika testów do tych TLPT.

Wiodący organ ds. TLPT koordynuje działania wszystkich organów ds. TLPT zaangażowanych w zbiorcze TLPT i podejmuje wszystkie decyzje niezbędne do przeprowadzenia zbiorczych TLPT w prawidłowy i skuteczny sposób.

6. W przypadku gdy organ ds. TLPT podmiotu finansowego zobowiązanego do przeprowadzenia TLPT różni się od jego właściwego organu, o którym mowa w art. 46 rozporządzenia (UE) 2022/2554, organy te, na potrzeby przeprowadzenia TLPT lub wykonywania swoich obowiązków zgodnie z tym rozporządzeniem, wymieniają się wszelkimi istotnymi informacjami dotyczącymi wszystkich kwestii związanych z TLPT.

Artykuł 17

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 lutego 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

Treść karty projektu (art. 9 ust. 2 lit. a))

Pozycja	Wymagane informacje
Osoba odpowiedzialna za plan projektu, tj. lider zespołu typu control team	Imię i nazwisko Dane kontaktowe
Testerzy	☐ wewnętrzni ☐ zewnętrzni ☐ wewnętrzni i zewnętrzni
Kanały komunikacji wybrane zgodnie z art. 9 ust. 2 lit. d) i art. 9 ust. 4 lit. a), w tym: a) stosowane szyfrowanie wiadomości e-mail b) wykorzystywane internetowe biura danych c) wykorzystywane komunikatory	
Kryptonim TLPT	
Ewentualne krytyczne lub istotne funkcje, które podmiot finansowy pełni w innych państwach członkowskich	1. wykaz krytycznych lub istotnych funkcji pełnionych w innym państwie członkowskim 2. w odniesieniu do każdej krytycznej lub istotnej funkcji – określenie państwa członkowskiego lub państw członkowskich, w których są one pełnione
Ewentualne krytyczne lub istotne funkcje wspierane przez zewnętrznych dostawców usług ICT	3. wykaz krytycznych lub istotnych funkcji wspieranych przez zewnętrznych dostawców usług ICT 4. w odniesieniu do każdej funkcji – określenie zewnętrznego dostawcy usług ICT
Przewidywane terminy zakończenia:	
1) etapu przygotowawczego, zgodnie z art. 9	rrrr-mm-dd
2) etapu testowania, zgodnie z art. 10 i 11	rrrr-mm-dd
3) etapu zamykania, zgodnie z art. 12	rrrr-mm-dd
4) planu naprawczego, zgodnie z art. 13	rrrr-mm-dd

ZAŁĄCZNIK II

Treść dokumentu określającego zakres (art. 9 ust. 6)

1. Dokument określający zakres zawiera wykaz wszystkich krytycznych lub istotnych funkcji zidentyfikowanych przez podmiot finansowy.

2. W odniesieniu do każdej zidentyfikowanej krytycznej lub istotnej funkcji podaje się następujące informacje:
   a) w przypadku gdy krytyczna lub istotna funkcja nie jest objęta zakresem TLPT – wyjaśnienie powodów, dla których nie została nim objęta;
   b) w przypadku gdy krytyczna lub istotna funkcja jest objęta zakresem TLPT:
      (i) wyjaśnienie powodów, dla których została nim objęta;
      (ii) zidentyfikowane systemy ICT wspierające tę krytyczną lub istotną funkcję;
      (iii) w odniesieniu do każdego zidentyfikowanego systemu ICT:
         1. czy usługi związane z tym systemem są zlecane w drodze outsourcingu, a jeżeli tak, nazwa zewnętrznego dostawcy usług ICT;
         2. jurysdykcje, w których system ICT jest wykorzystywany;
         3. wysokopoziomowy opis wstępnie wybranych flag, wskazujący, którego aspektu bezpieczeństwa – poufności, integralności, autentyczności czy dostępności – dotyczy każda flaga

ZAŁĄCZNIK III

Treść sprawozdania z ukierunkowanej analizy zagrożeń (art. 10 ust. 5)

Sprawozdanie z ukierunkowanej analizy zagrożeń zawiera informacje na temat wszystkich poniższych kwestii:

1. Ogólny zakres badań wywiadowczych obejmujący co najmniej następujące elementy:
   a) objęte zakresem krytyczne lub istotne funkcje;
   b) ich położenie geograficzne;
   c) używany język urzędowy UE;
   d) odpowiedni zewnętrzni dostawcy usług ICT;
   e) okres, w którym gromadzone są dana badawcze.
2. Ogólna ocena tego, jakie konkretne i użyteczne operacyjnie dane wywiadowcze można znaleźć na temat podmiotu finansowego, w tym:
   a) identyfikatory użytkownika i hasła pracowników;
   b) podobne domeny, które mogą być mylone z oficjalnymi domenami podmiotu finansowego;
   c) rozpoznanie techniczne: podatne na ataki lub exploity oprogramowanie, systemy i technologie;
   d) opublikowane w internecie przez pracowników informacje na temat podmiotu finansowego, które można wykorzystać na potrzeby ataku;
   e) informacje na sprzedaż w ciemnej sieci;
   f) wszelkie inne istotne informacje dostępne w internecie lub sieciach publicznych;
   g) w stosownych przypadkach – informacje na potrzeby fizycznego ataku, w tym sposoby dostępu do lokali podmiotu finansowego.
3. Analiza zagrożeń z uwzględnieniem ogólnego krajobrazu zagrożeń i szczególnej sytuacji podmiotu finansowego, w tym co najmniej:
   a) otoczenie geopolityczne;
   b) otoczenie gospodarcze;
   c) trendy technologiczne i wszelkie inne trendy związane z działalnością w sektorze usług finansowych.
4. Profile zagrożeń złośliwych podmiotów (konkretnego podmiotu/konkretnej grupy podmiotów lub ogólnej klasy), które mogą zaatakować podmiot finansowy, w tym systemy podmiotu finansowego, w przypadku których istnieje największe prawdopodobieństwo, że ich integralność zostanie naruszona przez złośliwe podmioty lub że staną się one celem ataku ze strony tych podmiotów, możliwa motywacja, zamiary i uzasadnienie potencjalnego ataku ze strony złośliwych podmiotów oraz możliwy sposób działania agresorów.
5. Scenariusze zagrożeń: co najmniej trzy kompleksowe scenariusze zagrożeń dla profili zagrożeń zidentyfikowanych zgodnie z pkt 4, które wykazują najwyższe poziomy krytyczności zagrożeń. Scenariusze zagrożenia opisują pełną ścieżkę ataku i obejmują co najmniej:
   a) jeden scenariusz obejmujący m.in. ograniczenie dostępności usług;
   b) jeden scenariusz obejmujący m.in. naruszenie integralności danych;
   c) jeden scenariusz obejmujący m.in. naruszenie poufności informacji.
6. W stosownych przypadkach opis scenariusza niezwiązanego z wyszukiwaniem istniejących zagrożeń, o którym mowa w art. 10 ust. 4.

ZAŁĄCZNIK IV

Treść planu testów z udziałem zespołu typu red team (art. 11 ust. 1)

Plan testów z udziałem zespołu typu red team zawiera informacje na temat wszystkich poniższych elementów, do których zaliczają się:

a) kanały i procedury komunikacji;

b) taktyki, techniki i procedury, których stosowanie w ataku jest dozwolone i niedozwolone, w tym granice etyczne dla inżynierii społecznej;

c) środki zarządzania ryzykiem, które mają być stosowane przez testerów;

d) opis każdego scenariusza, w tym:

   (i) symulowany agresor;

   (ii) jego zamiary, motywacja i cele;

   (iii) funkcje będące celem ataku lub wspierające je systemy ICT;

   (iv) aspekty poufności, integralności, dostępności i autentyczności będące celem ataku;

   (v) flagi;

e) szczegółowy opis każdej spodziewanej ścieżki ataku, w tym warunki wstępne i ewentualne ułatwienia, które ma zapewnić zespół typu control team, w tym terminy ich zapewnienia i potencjalne wykorzystanie;

f) harmonogram działań zespołu typu red team, w tym czas zaplanowany na realizację każdego scenariusza, podzielony co najmniej zgodnie z trzema etapami, które przechodzi tester w fazie testowania, a mianowicie wejściem do systemów ICT podmiotów finansowych, przejściem przez systemy ICT i wreszcie wykonaniem działań na celach i ostatecznym wydostaniem się z systemów ICT (etapy „wejścia", „przejścia" i „wyjścia");

g) szczególne cechy infrastruktury podmiotów finansowych, które należy uwzględnić podczas testów;

h) ewentualne dodatkowe informacje lub inne zasoby niezbędne testerom do realizacji scenariuszy.

ZAŁĄCZNIK V

Treść sprawozdania z testów sporządzanego przez zespół typu red team (art. 12 ust. 2)

Sprawozdanie z testów sporządzane przez zespół typu red team zawiera co najmniej wszystkie informacje, o których mowa poniżej:

a) informacje o przeprowadzonym ataku, w tym:
   (i) będące celem ataku krytyczne lub istotne funkcje oraz zidentyfikowane systemy, procesy i technologie ICT wspierające krytyczne lub istotne funkcję, określone w planie testów z udziałem zespołu typu red team;
   (ii) podsumowanie każdego scenariusza;
   (iii) zdobyte i niezdobyte flagi;
   (iv) ścieżki ataku, które zakończyły się sukcesem i porażką;
   (v) taktyki, techniki i procedury stosowane z powodzeniem i bez powodzenia;
   (vi) ewentualne odstępstwa od planu testów z udziałem zespołu typu red team;
   (vii) ewentualne przyznane ułatwienia;

b) wszystkie znane testerom działania, które zostały przeprowadzone przez zespół typu blue team w celu zrekonstruowania ataku i złagodzenia jego skutków;

c) wykryte podatności i inne ustalenia, w tym:
   (i) opis podatności i innych ustaleń, w tym ich krytyczności;
   (ii) analizę podstawowych przyczyn powodzenia ataków;
   (iii) zalecenia dotyczące środków zaradczych, w tym wskazanie ich hierarchii ważności.

ZAŁĄCZNIK VI

Treść sprawozdania z testów sporządzanego przez zespół typu blue team (art. 12 ust. 4)

Sprawozdanie z testów sporządzane przez zespół typu blue team zawiera co najmniej wszystkie informacje, o których mowa poniżej:

1. dla każdego etapu ataku opisanego przez testerów w sprawozdaniu z testów sporządzanym przez zespół typu red team:
   a) wykaz wykrytych prób ataku;
   b) wpisy w rejestrze odpowiadające tym wykryciom;
2. ocenę ustaleń i zaleceń testerów;
3. dowody ataku przeprowadzonego przez testerów zebrane przez zespół typu blue team;
4. dokonaną przez zespół typu blue team analizę podstawowych przyczyn powodzenia ataków ze strony testerów;
5. wykaz wyciągniętych wniosków i zidentyfikowanych możliwości poprawy;
6. wykaz tematów, którymi należy się zająć w ramach działań z udziałem zespołu typu purple team.

ZAŁĄCZNIK VII

Szczegóły sprawozdania podsumowującego istotne ustalenia TLPT, o którym mowa w art. 26 ust. 6 rozporządzenia (UE) 2022/2554

Sprawozdanie podsumowujące testy zawiera co najmniej wszystkie informacje, o których mowa poniżej:

a) zaangażowane strony;

b) plan projektu;

c) zatwierdzony zakres, w tym uzasadnienie objęcia bądź nieobjęcia nim krytycznych lub istotnych funkcji, oraz zidentyfikowane systemy, procesy i technologie ICT wspierające krytyczne lub istotne funkcje objęte TLPT;

d) wybrane scenariusze i wszelkie znaczące odstępstwa od sprawozdania z ukierunkowanej analizy zagrożeń;

e) zrealizowane ścieżki ataku oraz zastosowane taktyki, techniki i procedury;

f) zdobyte i niezdobyte flagi;

g) ewentualne odstępstwa od planu testów z udziałem zespołu typu red team;

h) ewentualne wykrycia przez zespół typu blue team;

i) działania z udziałem zespołu typu purple team w fazie testowania, jeżeli zostały przeprowadzone, i związane z tym warunki;

j) ewentualne ułatwienia;

k) wprowadzone środki zarządzania ryzykiem;

l) zidentyfikowane podatności i inne ustalenia, w tym ich krytyczność;

m) analizę podstawowych przyczyn powodzenia ataków;

n) wysokopoziomowy plan dotyczący środków zaradczych, łączący podatności na zagrożenia i inne ustalenia, ich podstawowe przyczyny i hierarchię ważności działań zaradczych;

o) wnioski wyciągnięte z otrzymanych informacji zwrotnych.

ZAŁĄCZNIK VIII

Szczegóły poświadczenia przeprowadzenia TLPT, o którym mowa w art. 26 ust. 7 rozporządzenia (UE) 2022/2554

Poświadczenie zawiera co najmniej wszystkie następujące informacje:

a) w odniesieniu do przeprowadzonych TLPT:

(i) datę rozpoczęcia i zakończenia TLPT;

(ii) krytyczne lub istotne funkcje objęte zakresem testów;

(iii) w stosownych przypadkach – informacje na temat krytycznych lub istotnych funkcji objętych zakresem testów, w odniesieniu do których nie przeprowadzono TLPT;

(iv) w stosownych przypadkach – informacje na temat innych podmiotów finansowych, które były zaangażowane w TLPT;

(v) w stosownych przypadkach – informacje na temat zewnętrznych dostawców usług ICT, którzy brali udział w TLPT;

(vi) w odniesieniu do testerów informacje o tym, czy:

1. korzystano z testerów wewnętrznych;

2. podmiot finansowy skorzystał z możliwości, o której mowa w art. 5 ust. 3 akapit drugi;

(vii) czas trwania, w dniach kalendarzowych, etapu aktywnego testowania z udziałem zespołu typu red team;

b) w przypadku gdy w TLPT było zaangażowanych kilka organów ds. TLPT – informacje na temat pozostałych organów ds. TLPT i charakteru, w jakim były one zaangażowane;

c) wykaz dokumentów przeanalizowanych przez organ ds. TLPT do celów wydania poświadczenia.