Przegląd Bezpieczeństwa Wewnętrznego

2026, nr 34, s. 13–35

 https://doi.org/10.4467/20801335PBW.26.001.23363

ARTYKUŁ

Testy threat-led penetration testing (TLPT) – nowe podejście do testowania cyfrowej odporności podmiotów finansowych w Polsce w kontekście obowiązków wynikających z rozporządzenia Digital Operational Resilience Act (DORA)

Threat-led penetration testing (TLPT) – a new approach to testing digital resilience of financial entities in Poland in the perspective of requirements under the Digital Operational Resilience Act (DORA)

KAMIL MROCZKA

Wydział Nauk Politycznych i Studiów Międzynarodowych,
Uniwersytet Warszawski

https://orcid.org/0000-0003-3809-3479

PAWEŁ PIEKUTOWSKI

Departament Cyberbezpieczeństwa,
Urząd Komisji Nadzoru Finansowego

https://orcid.org/0009-0001-5861-7367

Abstrakt

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA) wprowadziło do unijnego, a tym samym i krajowego, porządku prawnego nowy model testowania cyfrowej odporności podmiotów finansowych działających na polskim rynku finansowym. Zasadniczym celem artykułu jest omówienie i ocena modelu threat-led penetration

testing (TLPT), czyli testów penetracyjnych opartych na zagrożeniach. Testy TLPT mogą obejmować zarówno techniczne, jak i socjotechniczne elementy. Hipotezą artykułu jest twierdzenie, że testy TLPT powinny wpłynąć pozytywnie na zwiększanie cyfrowej odporności podmiotów finansowych, gdyż są zaprojektowane tak, aby imitować rzeczywiste cyberataki, co umożliwia organizacjom zrozumienie swojej odporności na zagrożenia oraz podjęcie odpowiednich działań naprawczych. Uzyskane rezultaty analizy potwierdzają postawioną hipotezę badawczą. Wynika to z faktu, że głównym założeniem testów TLPT jest jak najwierniejsze odzwierciedlenie rzeczywistych scenariuszy ataków. Stwarza to możliwość bardziej rzetelnej i szczegółowej oceny poziomu bezpieczeństwa organizacji. Autorzy podkreślają, że takie podejście pozwala nie tylko na weryfikację skuteczności zabezpieczeń infrastruktury teleinformatycznej, lecz także na ocenę odporności procesów operacyjnych oraz poziomu świadomości pracowników w obszarze cyberzagrożeń.

Słowa kluczowe testy TLPT, DORA, Komisja Nadzoru Finansowego, cyfrowa odporność, cyberbezpieczeństwo

Abstract Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA) launched a new model for testing the digital resilience of financial services operating in the Polish financial market into the EU and thus into the domestic legal framework. The primary purpose of this article is to discuss and evaluate the Threat-Led Penetration Testing (TLPT) model. TLPT tests can include both technical and sociotechnical components. The hypothesis of the article is that TLPT testing will have a positive impact on enhancing the digital resilience of financial stakeholders because these tests are designed to simulate real-world cyber attacks, enabling organisations to understand their resilience to threats and initiate relevant countermeasures. The results obtained from the analysis confirm the validity of the proposed research hypothesis. This follows from the fact that the fundamental premise of TLPT testing is to replicate real-world attack scenarios as accurately as possible, thereby enabling a more reliable and detailed assessment of organisation's security posture. The authors emphasise that such an approach allows not only for the verification of the effectiveness of information system safeguards, but also for the evaluation of the resilience of operational processes and the level of employee awareness regarding cyber threats.

Keywords TLPT tests, DORA, Polish Financial Supervision Authority, digital resilience, cybersecurity

Wprowadzenie

Technologie informacyjno-komunikacyjne (information and communication technologies, ICT[1]) są obecne niemal w każdym obszarze funkcjonowania państw i ich gospodarek[2]. Stanowią realne wsparcie dla złożonych systemów wykorzystywanych w codziennych działaniach. Technologie te napędzają polską gospodarkę i jej najważniejsze sektory, w tym sektor finansowy, oraz wzmacniają funkcjonowanie rynku wewnętrznego Unii Europejskiej. Gęstniejąca sieć wzajemnych powiązań między interesariuszami rynku finansowego, dostawcami usług finansowych i klientami tego rynku wraz z postępującą cyfryzacją systemów finansowych zwiększają podatność na różnego rodzaju ryzyko, w tym wynikające z cyberzagrożeń i zakłóceń w funkcjonowaniu ICT. Niezbędne jest zatem podejmowanie działań mających na celu zwiększanie odporności cyfrowej podmiotów finansowych.

W motywie 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (dalej: rozporządzenie DORA)[3] jednoznacznie podkreślono, że (…) *w ostatnich dziesięcioleciach korzystanie z ICT zaczęło odgrywać zasadniczą rolę, jeżeli chodzi o świadczenie usług finansowych, do tego stopnia, że obecnie ICT mają krytyczne znaczenie dla wykonywania typowych codziennych funkcji wszystkich podmiotów finansowych*. W piśmiennictwie słusznie się zauważa, że obowiązujące od stycznia 2025 r. rozporządzenie DORA zobowiązało podmioty finansowe oraz zewnętrznych dostawców usług ICT do stosowania najlepszych praktyk w zakresie cyberbezpieczeństwa. Za jeden z zaawansowanych środków prowadzących do zwiększenia odporności cyfrowej podmiotów finansowych uznano testy penetracyjne oparte na zagrożeniach (threat-led penetration testing, TLPT). Będą one wykorzystywane do oceny stanu cyberbezpieczeństwa tych podmiotów[4].

Nie wchodząc w tym miejscu w pogłębioną analizę zakresu znaczeniowego terminu „threat-led penetration testing", należy podkreślić, że jest to technika oceny

---

[1] Wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego (przyp. red.).

[2] W artykule wykorzystano publikację jednego z autorów przygotowaną na potrzeby procesu wdrażania rozporządzenia DORA. Zob. *Testy TLPT – nowe podejście do testowania cyfrowej odporności organizacji*, Komisja Nadzoru Finansowego, 14 VII 2025 r., https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [dostęp: 9 II 2026].

[3] *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*.

[4] M.L. Dozsa, *Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, praca magisterska, Oslo 2024, s. ii.

cyberbezpieczeństwa służąca do symulacji realistycznych scenariuszy cyberataków, których celem są krytyczne systemy i infrastruktura organizacji. W przeciwieństwie do tradycyjnych testów penetracyjnych, mogących opierać się na standardowej liście podatności, metoda TLPT koncentruje się na naśladowaniu konkretnych aktorów, technik i taktyk, których zaistnienie w organizacji jest najbardziej prawdopodobne ze względu na jej unikalny profil ryzyka. Testy TLPT są przeprowadzane, aby zidentyfikować słabości, zweryfikować istniejące środki bezpieczeństwa i zwiększyć zdolności organizacji do wykrywania rzeczywistych cyberzagrożeń, reagowania na nie i odzyskiwania danych[5].

Głównym celem artykułu jest krytyczna analiza modelu TLPT jako instrumentu oceny cyfrowej odporności podmiotów finansowych w Polsce w kontekście wymogów rozporządzenia DORA, ze szczególnym uwzględnieniem różnic między testami TLPT a klasycznymi testami penetracyjnymi, roli instytucji nadzorczych oraz implikacji wdrożeniowych.

Autorzy artykułu przyjęli następującą hipotezę: testy TLPT powinny wpłynąć pozytywnie na zwiększanie cyfrowej odporności podmiotów finansowych, gdyż są zaprojektowane tak, aby imitować rzeczywiste cyberataki, co umożliwia organizacjom zrozumienie swojej odporności na zagrożenia oraz podjęcie odpowiednich działań naprawczych.

Na potrzeby prowadzonych rozważań wykorzystano metodę prawnoporównawczą, analizę instytucjonalną oraz krytyczną analizę piśmiennictwa naukowego. Zastosowano również obserwację uczestniczącą wynikającą z doświadczeń zawodowych autorów. Wskazane metody pozwoliły na ustalenie roli i kompetencji podmiotów odpowiedzialnych za cyberbezpieczeństwo rynku finansowego, a także na identyfikację różnic w podejściu do testowania odporności cyfrowej, ocenę stopnia harmonizacji regulacyjnej oraz zasygnalizowanie obszarów, w których polski model nadzoru nad cyberbezpieczeństwem rynku finansowego może wymagać doprecyzowania lub dalszego rozwoju.

Testy TLPT – definicja

Definiując testy TLPT, eksperci z zakresu cyberbezpieczeństwa podkreślają, że jest to (…) *zaawansowana forma testów penetracyjnych, która wykracza poza standardowe podejście, symulując rzeczywiste ataki cybernetyczne z wykorzystaniem taktyk, technik i procedur (TTP) stosowanych przez prawdziwych cyberprzestępców.*

[5] B. Riaz, Z. Younas, *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024, s. 26.

W przeciwieństwie do tradycyjnych testów penetracyjnych, TLPT koncentruje się na analizie konkretnych zagrożeń, na które narażona jest dana organizacja, dostosowując symulacje ataków do jej specyficznego profilu ryzyka[6].

Definicję legalną testów TLPT zawarto w art. 3 pkt 17 rozporządzenia DORA. Zgodnie z tym przepisem testy te oznaczają (…) *ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają dostarczenie kontrolowanych, dostosowanych do podmiotu, wynikających z analizy zebranych danych (red team) testów działających na bieżąco krytycznych systemów produkcyjnych podmiotu finansowego*[7].

Testy penetracyjne a testy TLPT – najważniejsze różnice

Głównym celem realizacji testów TLPT jest ocena realnej odporności instytucji na zagrożenia i mogące zaistnieć scenariusze ataków. Test penetracyjny skupia się bardziej na identyfikacji technicznych podatności i błędów konfiguracyjnych w systemach informatycznych.

Uszczegóławiając, można wskazać następujące różnice:

1) zakres realizacji testu – testy penetracyjne koncentrują się zazwyczaj na ściśle określonych elementach infrastruktury IT – pojedynczych systemach, aplikacjach czy komponentach sieci. Ich celem jest przede wszystkim wykrycie podatności technicznych w zdefiniowanym obszarze. To podejście pozwala na ocenę bezpieczeństwa konkretnego systemu, ale nie daje pełnego obrazu, jak organizacja poradziłaby sobie ze złożonym cyberatakiem. W testach TLPT podchodzi się do tematu znacznie szerzej. Obejmują one nie tylko systemy i technologie, lecz także procesy operacyjne i ludzi. Celem jest sprawdzenie całego ekosystemu cyberobrony organizacji i odpowiedź na pytania: jak działa monitorowanie bezpieczeństwa? Jak przebiega komunikacja wewnętrzna? Jak zespół reaguje na incydenty? Jakie są ścieżki eskalacji? Testy TLPT pozwalają zobaczyć, czy organizacja jest przygotowana na atak nie tylko teoretycznie, lecz także w praktyce. Umożliwia to zwiększenie odporności całego „organizmu", a nie tylko pojedynczego elementu;

---

[6] *Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA*, Bankowe ABC, 2 I 2025 r., https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [dostęp: 19 IV 2025].

[7] Zob. także: J. Kurek-Sobieraj, Komentarz do art. 3, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 85–86.

2) scenariusze ataków – testy penetracyjne opierają się głównie na znanych podatnościach i skupiają się bardziej na identyfikacji potencjalnych zagrożeń w określonym systemie informatycznym. Testy TLPT są realizowane na podstawie scenariuszy opracowanych przez specjalny zespół threat intelligence. Ma on zidentyfikować najbardziej realistyczne cyberzagrożenia i scenariusze ataków, z którymi może mieć do czynienia dana organizacja. Scenariusze te mogą bazować na raportach dotyczących ogólnej analizy cyberzagrożeń (generic threat intelligence) dla danego sektora. W raporcie opublikowanym przez zespół reagowania na incydenty bezpieczeństwa komputerowego Komisji Nadzoru Finansowego (CSIRT KNF) zostały opisane potencjalne rodzaje ataków, kategorie adwersarzy i trendy w realizacji cyberataków[8]. Duży nacisk położono w nim na możliwy rozwój zagrożeń związanych z wykorzystaniem technik i narzędzi opartych na sztucznej inteligencji, a także na niebezpieczeństwa wynikające z ataków na łańcuchy dostaw. Istotnymi aspektami są również intensyfikacja ataków ransomware, coraz częściej realizowanych w modelu ransomware as a service, oraz rozwój zjawiska haktywizmu, który przybrał na sile po wybuchu wojny w Ukrainie;
3) środowisko testowe i podejście do ryzyka – testy penetracyjne są realizowane najczęściej w odpowiednich środowiskach testowych, aby uniknąć zakłóceń w funkcjonowaniu systemów. W testach TLPT duży nacisk jest położony na kompleksowe zbadanie faktycznego poziomu bezpieczeństwa organizacji, dlatego są one przeprowadzane na środowiskach produkcyjnych. Oznacza to dodatkowe ryzyko związane z możliwością zakłócenia ciągłości działania systemów i procesów biznesowych. W związku z tym podczas testów TLPT niezbędne jest prowadzenie analizy ryzyka pozwalającej na mitygację zakłóceń, które mogłyby się pojawić podczas ich realizacji;
4) przebieg testów i poufność – cechą charakterystyczną testów TLPT jest wymóg zachowania ich w tajemnicy przed większością organizacji. Jedynie wąska grupa pracowników ma świadomość ich realizacji. Intencją jest zweryfikowanie reakcji organizacji na cyberzagrożenie. Bada się nie tylko cyfrową odporność systemów teleinformatycznych, lecz także przygotowanie zespołów bezpieczeństwa oraz funkcjonowanie odpowiednich procesów wewnątrz organizacji. Zachowanie poufności testów stanowi duże wyzwanie dla organizacji ze względu na złożoność wielu procesów biznesowych;

[8] *Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025*, CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [dostęp: 19 I 2026].

5) wyniki i raportowanie – istotnym elementem realizacji testów TLPT są ćwiczenia typu purple team, które odbywają się po zakończeniu fazy ataków. Są to ćwiczenia, w ramach których zespół symulujący ataki oraz zespół odpowiedzialny za obronę wspólnie omawiają przeprowadzone scenariusze, identyfikują słabości w procesach i systemach, a także wypracowują rozwiązania pozwalające na zwiększenie poziomu cyberodporności organizacji. Następnie jest przygotowywany plan działań naprawczych;
6) częstotliwość testu – testy penetracyjne mogą być realizowane z większą częstotliwością. Testy TLPT są przeprowadzane zdecydowanie rzadziej ze względu na poziom ich skomplikowania oraz koszty.

Obowiązek testowania cyfrowej odporności podmiotów finansowych w świetle art. 26 rozporządzenia DORA

Rozporządzenie DORA zobowiązuje podmioty finansowe (z pewnymi wyłączeniami wskazanymi w art. 16 ust. 1 akapit pierwszy rozporządzenia DORA) do przeprowadzania testów TLPT nie rzadziej niż co trzy lata. Na podstawie profilu ryzyka danego podmiotu finansowego i z uwzględnieniem okoliczności operacyjnych właściwy organ może jednak, w razie potrzeby, zwrócić się do tego podmiotu o zmniejszenie lub zwiększenie częstotliwości przeprowadzania testów TLPT. W piśmiennictwie stwierdza się, że może to nastąpić w przypadku (…) *pozyskania przez właściwy organ uzasadnionych podejrzeń, że w organizacji doszło do nieprawidłowego zarządzania ryzykiem (np. przez pojawienie się ofert sprzedaży danych organizacji na czarnym rynku)*[9].

Niezwykle ważny z perspektywy wymagań dotyczących jakości jest ust. 2 przywołanego przepisu. Stanowi on, że: *każdy test penetracyjny ukierunkowany przez analizę zagrożeń obejmuje kilka krytycznych lub istotnych funkcji podmiotu finansowego lub wszystkie te funkcje i jest przeprowadzany na działających systemach produkcyjnych wspierających takie funkcje.* Pierwszym krokiem do rzetelnego przeprowadzenia testów TLPT jest określenie wszelkich stosownych systemów bazowych. Następnie podmioty finansowe powinny ustalić wszystkie procesy i technologie ICT wspierające krytyczne lub istotne funkcje. Ostatnie działanie polega na określeniu, które usługi ICT, w tym systemy, procesy i technologie ICT wspierające krytyczne lub istotne funkcje i usługi, zostały zlecone w drodze outsourcingu zewnętrznym dostawcom usług ICT lub są przedmiotem umowy z takimi dostawcami.

[9] C. Cichocki, Komentarz do art. 26, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 280.

W doktrynie słusznie podkreśla się, że profesjonalny proces gromadzenia tych informacji i danych wymaga wiedzy biznesowej o funkcjonowaniu organizacji oraz przełożenia jej na wiedzę technologiczną i techniczną. Do takich działań można wykorzystać różne narzędzia ICT, np. systemy klasy CMDB (computer management database)[10]. W praktyce badanie może dotyczyć wszystkich lub tylko wybranych systemów czy funkcjonalności. Mając na uwadze wysoki poziom współzależności systemów i narzędzi ICT w podmiotach finansowych, zaleca się kompleksowe badania. Na podstawie informacji i danych uzyskanych z analizy podmioty te mają obowiązek dokonania oceny, które krytyczne lub istotne funkcje należy objąć testami TLPT. Ocenę tę zatwierdzają właściwe organy. W polskim porządku prawnym jest to Komisja Nadzoru Finansowego, o czym będzie mowa w dalszej części artykułu.

W przypadku gdy zakres TLPT obejmuje zewnętrznych dostawców usług ICT, podmiot finansowy stosuje niezbędne środki i zabezpieczenia, aby wzięli oni udział w testach, i przez cały czas ponosi pełną odpowiedzialność za zapewnianie zgodności z rozporządzeniem DORA. Wymóg ten jest krytycznie istotny w kontekście praktyki funkcjonowania podmiotów finansowych, gdyż wszystkie korzystają z usług zewnętrznych dostawców.

Prawodawca unijny, świadomy skali działania dostawców usług ICT, wprowadza pewne odstępstwa od generalnej zasady ich udziału w testach TLPT. Zgodnie z brzmieniem art. 26 ust. 4 rozporządzenia DORA:

> (…) w przypadku gdy można racjonalnie przewidywać, że udział zewnętrznego dostawcy usług ICT w TLPT (…) będzie miał negatywny wpływ na jakość lub bezpieczeństwo usług świadczonych przez tego zewnętrznego dostawcę usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia lub na poufność danych związanych z takimi usługami, dany podmiot finansowy i dany zewnętrzny dostawca usług ICT mogą uzgodnić na piśmie, że ten zewnętrzny dostawca usług ICT zawrze ustalenia umowne bezpośrednio z testerem zewnętrznym w celu przeprowadzenia – pod kierownictwem jednego wyznaczonego podmiotu finansowego – zbiorczych TLPT z udziałem kilku podmiotów finansowych (testowania zbiorczego), na rzecz których dany zewnętrzny dostawca usług ICT świadczy usługi ICT.
>
> Takie testowanie zbiorcze obejmuje odpowiedni zakres usług ICT wspierających krytyczne lub istotne funkcje będące przedmiotem zawartej przez te podmioty finansowe umowy z tym zewnętrznym dostawcą usług ICT. Testowanie zbiorcze uznaje się za TLPT przeprowadzone przez podmioty finansowe biorące udział w tym testowaniu zbiorczym.

[10] Tamże.

Liczba podmiotów finansowych uczestniczących w takim testowaniu jest odpowiednio dostosowana i uwzględnia stopień złożoności i rodzaj usług nim objętych. Po zakończeniu testów, uzgodnieniu sprawozdań i planów naprawczych podmiot finansowy i w stosownych przypadkach testerzy zewnętrzni przedstawiają właściwemu organowi podsumowanie ustaleń, plany naprawcze i dokumentację wykazującą, że testy przeprowadzono zgodnie z wymogami rozporządzenia. Na tej podstawie właściwe organy wydają podmiotom finansowym poświadczenie, które potwierdza przeprowadzenie testów zgodnie z wymaganiami określonymi w dokumentacji. Umożliwia ono organom wzajemne uznawanie testów TLPT, przy czym nie zwalnia podmiotów finansowych z odpowiedzialności za wyniki tych testów.

Na podmioty finansowe nałożono obowiązek zawarcia umów, których celem jest przeprowadzenie testów TLPT. Jeżeli podmiot finansowy dysponuje zespołami testerów wewnętrznych, rozporządzenie DORA nakłada wymóg zrealizowania tego rodzaju testów przez testera zewnętrznego co trzy testy, czyli najrzadziej co dziewięć lat. Wyjątek od tej zasady dotyczy instytucji kredytowych sklasyfikowanych jako istotne zgodnie z art. 6 ust. 4 rozporządzenia Rady UE nr 1024/2013[11]. Podmioty te mają obowiązek korzystania wyłącznie z testerów zewnętrznych.

Rozporządzenie DORA definiuje również kryteria, które są stosowane przez właściwe organy do określania podmiotów objętych obowiązkiem testowania TLPT. W ocenie uwzględnia się:

- czynniki związane z wpływem, zwłaszcza zakres, w jakim świadczone usługi i działania podejmowane przez podmiot finansowy mają wpływ na sektor finansowy,
- ewentualne obawy dotyczące stabilności finansowej, w tym systemowy charakter podmiotu finansowego na poziomie unijnym lub krajowym,
- specyficzny profil ryzyka związanego z ICT, poziom zaawansowania podmiotu finansowego pod względem ICT lub zastosowane rozwiązania technologiczne.

Syntetyzując analizę przedmiotową i podmiotową art. 26 rozporządzenia DORA, należy wskazać, że przepis ten daje państwom członkowskim możliwość wyznaczenia jednego organu publicznego w sektorze finansowym, który na szczeblu krajowym będzie odpowiedzialny za kwestie związane z testami TLPT w tym sektorze. Organowi temu powierza się wszystkie kompetencje i zadania w tym zakresie.

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

Wymogi dotyczące testerów zewnętrznych i wewnętrznych

W art. 27 rozporządzenia DORA zostały zdefiniowane podstawowe wymagania dotyczące testerów przeprowadzających testy TLPT. Ustęp 1 tego przepisu stanowi, że podmioty finansowe korzystają w tym przypadku wyłącznie z usług testerów zewnętrznych, którzy:

a) są najbardziej odpowiedni do tego zadania i cieszą się największą renomą;
b) posiadają zdolności techniczne i organizacyjne oraz wykazują się szczególną wiedzą fachową w zakresie analizy zagrożeń, testów penetracyjnych i testów z udziałem zespołów typu red team;
c) posiadają certyfikat wydany przez jednostkę akredytującą w państwie członkowskim lub przystąpili do formalnych kodeksów postępowania lub ram etycznych;
d) przedstawiają niezależne zapewnienie lub sprawozdanie z audytu dotyczące należytego zarządzania ryzykiem związanym z przeprowadzaniem TLPT, w tym należytej ochrony poufnych informacji podmiotu finansowego i mitygacji ryzyka biznesowego podmiotu finansowego;
e) są należycie i w pełni objęci odpowiednimi ubezpieczeniami od odpowiedzialności cywilnej z tytułu wykonywania zawodu, w tym od ryzyka uchybień i zaniedbań.

W doktrynie słusznie podkreśla się, że (…) *trafność i rzetelność testów TLPT jest traktowana przez ustawodawcę jako kluczowa, bowiem poszczególne organizacje finansowe powinny ufać certyfikatom okazywanym przez inne podmioty z branży. Również dla organu właściwego dla kontroli, istotny jest poziom zaufania do testerów zewnętrznych lub wewnętrznych*[12].

Prawodawca unijny dopuszcza możliwość korzystania z testerów wewnętrznych. Stawia jednak dodatkowe wymogi, poza przywołanymi powyżej w odniesieniu do testerów zewnętrznych. W art. 27 ust. 2 rozporządzenie DORA stanowi, że podmioty finansowe korzystające z testerów wewnętrznych zapewniają spełnienie następujących warunków:

a) takie korzystanie z testerów wewnętrznych zostało zatwierdzone przez odpowiedni właściwy organ lub przez jeden organ publiczny wyznaczony zgodnie z art. 26 ust. 9 i 10;
b) odpowiedni właściwy organ sprawdził, że dany podmiot finansowy dysponuje wystarczającymi zasobami przeznaczonymi na ten cel i że zapewnił unikanie konfliktów interesów na wszystkich etapach projektowania i wykonywania testu; oraz

[12] C. Cichocki, Komentarz do art. 27, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 284.

c) dostawca analizy zagrożeń jest podmiotem zewnętrznym względem danego podmiotu finansowego.

W art. 27 ust. 3 rozporządzenia DORA zwraca się uwagę na kwestie bezpieczeństwa informacji i danych wynikających z testów TLPT. Podmioty finansowe mają zapewnić, aby umowy zawarte z testerami zewnętrznymi zobowiązywały tych testerów do (…) *należytego zarządzania wynikami TLPT oraz aby żadne przetwarzanie danych pochodzących z tych wyników, w tym generowanie, przechowywanie, agregowanie, sporządzanie, zgłaszanie, przekazywanie lub niszczenie, nie stwarzały ryzyka dla podmiotu finansowego*.

Cezary Cichocki słusznie podnosi, że dane uzyskane w wyniku testów TLPT należy traktować jako szczególnie wrażliwe z uwagi na to, że jeśli (…) *wpadną w ręce osób niepowołanych, to stanowić będą rodzaj przewodnika po podatnościach w systemach organizacji finansowej i znacznie ułatwią potencjalnemu intruzowi atak. Ryzyko ujawnienia tych danych polega na tym, że pomiędzy ujawnieniem zagrożeń w ramach testów TLPT a ich mitygacją może minąć pewien interwał czasu, który stanie się oknem ataku w wypadku ujawnienia danych z testów osobom nieuprawnionym*[13].

Testowanie cyfrowej odporności podmiotów finansowych na gruncie prawa krajowego

Rozporządzenie DORA wykreowało nowe otoczenie regulacyjne dla podmiotów finansowych oraz KNF jako organu odpowiedzialnego za nadzór nad jego przestrzeganiem. Przepisy rozporządzenia są stosowane bezpośrednio, jednak niektóre z nich wymagają wprowadzenia zmian w krajowym porządku prawnym, zwłaszcza w odniesieniu do wyznaczenia organów właściwych oraz nałożenia obowiązków na podmioty finansowe[14].

Pierwszy projekt ustawy wdrażający przywołane regulacje prawa unijnego został przedłożony przez Ministra Finansów w kwietniu 2024 r.[15] Proces legislacyjny trwał ponad rok, co budzi pytania w kontekście pilności wprowadzenia tej regulacji. Opieszałość decydentów spowodowała, że pod koniec marca 2025 r. Komisja Europejska

[13] Tamże, s. 285.

[14] *Ustawa wdrażająca DORA do prawa polskiego*, „Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [dostęp: 12 IV 2025].

[15] *Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji*, druk nr UC11, Rządowe Centrum Legislacji, Warszawa 2025.

wezwała Polskę i 12 innych państw unijnych do pełnego wdrożenia rozporządzenia DORA w ramach krajowych systemów prawnych[16]. Rządowy proces legislacyjny zakończył się w kwietniu 2025 r. Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego został zaakceptowany przez Stały Komitet Rady Ministrów. Ustawę wdrażającą rozporządzenie DORA uchwalono w czerwcu 2025 r.[17]

Z perspektywy celu tego artykułu najważniejsze zmiany dotyczą wprowadzenia art. 18zk do *Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym*. Przepis ten reguluje zadania KNF w zakresie przeprowadzenia testów, o których mowa w art. 26 rozporządzenia DORA, oraz sposób postępowania podmiotów finansowych zobowiązanych do ich przeprowadzania. Na mocy tego przepisu organ nadzoru stał się organem odpowiedzialnym za realizację obowiązków organu właściwego, wskazanych w art. 26 i art. 27 rozporządzenia DORA. W świetle powyższego KNF wyposażono w ustawowe uprawnienie do wyznaczania – w drodze decyzji – podmiotu finansowego zobowiązanego do przeprowadzenia testów TLPT. Artykuł 18zk powiela kryteria wyboru podmiotów obowiązanych do przeprowadzenia tych testów z uwzględnieniem zasady proporcjonalności (art. 4 ust. 2 rozporządzenia DORA).

Podmioty, w stosunku do których KNF wydała wspomnianą decyzję, są zobowiązane do przekazywania organowi nadzoru, w celu zatwierdzenia, wyniku oceny dokonanej zgodnie z art. 26 ust. 2 akapit trzeci rozporządzenia DORA. Wynik ten wskazuje, które krytyczne lub istotne funkcje należy objąć testami TLPT. Po ich przeprowadzeniu, uzgodnieniu sprawozdań i planów naprawczych podmiot finansowy i – w stosownych przypadkach – testerzy zewnętrzni będą zobowiązani do przedstawienia KNF podsumowania ustaleń, planów naprawczych i dokumentacji potwierdzającej, że testy TLPT zostały zrealizowane zgodnie z wymogami rozporządzenia DORA. Obowiązkiem organu nadzoru – w świetle art. 18zk ust. 4 – będzie potwierdzanie tej zgodności. Ma to umożliwić wzajemne uznawanie testów penetracyjnych przez właściwe organy.

Komisji Nadzoru Finansowego przyznano również kompetencje w zakresie zmniejszania lub zwiększenia częstotliwości przeprowadzania testów TLPT oraz legitymację do zatwierdzania zamiaru korzystania przez podmiot finansowy z usług testerów wewnętrznych. Jej odpowiedzialnością jest ponadto weryfikacja, czy testerzy wewnętrzni spełniają wymagania rozporządzenia DORA. Realizacja tego

[16] Na liście państw, które nie wdrożyły rozporządzenia, znalazły się również: Belgia, Bułgaria, Dania, Grecja, Hiszpania, Francja, Litwa, Łotwa, Malta, Portugalia, Rumunia i Słowenia.

[17] *Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji*.

obowiązku – w świetle nieostrych wymagań art. 27 rozporządzenia DORA – może powodować istotne problemy. Można jednak założyć, że w interesie podmiotów finansowych leży zapewnienie odpowiedniej jakości zasobów do realizacji testów TLPT. Jakość tych testów wpływa bowiem na zwiększenie poziomu odporności cyfrowej, a tym samym na szeroko pojęte bezpieczeństwo podmiotu finansowego.

Regulacyjne standardy techniczne w zakresie testów TLPT

W art. 26 ust. 11 rozporządzenia DORA prawodawca unijny zdecydował, że europejskie urzędy nadzoru (EUN) w porozumieniu z Europejskim Bankiem Centralnym opracują wspólne projekty regulacyjnych standardów technicznych (regulatory technical standards, RTS)[18] zgodne z ramami frameworku TIBER-EU (European framework for threat intelligence-based ethical red teaming). W RTS mają zostać doprecyzowane następujące elementy:

- kryteria wykorzystywane do celów stosowania ust. 8 akapit drugi rozporządzenia DORA,
- kryteria określające sposoby identyfikacji i notyfikacji podmiotów zobowiązanych do realizacji testów TLPT,
- role i obowiązki poszczególnych zespołów uczestniczących w testach,
- wymogi i standardy regulujące korzystanie z testerów wewnętrznych,
- wymogi dotyczące:
  - zakresu TLPT,
  - metodyki testowania i podejścia, które należy stosować na każdym konkretnym etapie testowania,
  - etapów testów odnoszących się do wyników, zamykania testów oraz środków naprawczych,
- rodzaj współpracy w zakresie nadzoru i inne odpowiednie rodzaje współpracy potrzebne do przeprowadzenia testów TLPT i do ułatwienia wzajemnego uznawania takiego testowania w kontekście podmiotów finansowych, które działają w więcej niż jednym państwie członkowskim. Ma to umożliwić odpowiedni poziom zaangażowania organów nadzoru i elastyczne

[18] Regulacyjne standardy techniczne nakładają szczegółowe wymagania techniczne dotyczące wdrożenia przepisów. Są bardziej normatywne i koncentrują się na praktycznych aspektach implementacji rozporządzenia DORA. Z kolei wykonawcze standardy techniczne (implementing technical standards, ITS) zajmują się ujednoliceniem i standaryzacją procesów wdrażania tych przepisów w UE i mają charakter bardziej proceduralny. Skupiają się dużo bardziej na odpowiednim sposobie raportowania do właściwych organów nadzoru.

wdrażanie, uwzględniające specyfikę podsektorów finansowych lub lokalnych rynków finansowych.

W lipcu 2024 r. EUN zaprezentowały finalny raport z konsultacji RTS w sprawie testów TLPT[19].

Testy TLPT a TIBER-EU

Zanim zostaną omówione zależności między testami TLPT a TIBER-EU[20], konieczne jest krótkie scharakteryzowanie założeń tego dokumentu. Framework TIBER-EU został powołany w 2018 r. przez Europejski Bank Centralny w celu usystematyzowania i ujednolicenia podejścia i realizacji realistycznych testów penetracyjnych w organizacjach z sektora finansowego państw członkowskich UE[21]. TIBER-EU definiuje model testów/operacji red teamowych poprzedzonych przeprowadzeniem rozpoznania i analizy danych na temat zagrożeń ukierunkowanych na testowany podmiot. Stanowi on fundament wymagań dotyczących realizacji testów TLPT. W początkowym etapie istniały różnice pomiędzy założeniami tego dokumentu a wymaganiami określonymi w rozporządzeniu DORA. Główna polegała na odmiennym podejściu do przeprowadzania testów z udziałem testerów wewnętrznych. TIBER-EU pierwotnie nie dopuszczał takiego rozwiązania, a w testach TLPT jest ono akceptowalne pod warunkiem spełnienia określonych kryteriów. Framework TIBER-EU został zaktualizowany w 2025 r. i jego obecna wersja odzwierciedla wymagania wynikające z rozporządzenia DORA[22]. Można zatem uznać, że aktualny TIBER-EU to podręcznik do realizacji testów TLPT. Podczas gdy

[19] *Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554*, European Banking Authority, 17 July 2024.

[20] Na temat założeń TIBER-EU zob. szerzej: T. Valkeasuo, *TIBER-EU Preparation Phase Framework. Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023; M. Bayle de Jessé, *The Eurosystem's cyber resilience strategy for financial market infrastructures*, „Cyber Security: A Peer-Reviewed Journal" 2019, t. 2, nr 4, s. 294–302. https://doi.org/10.69554/DFBJ2963; B.F. Scott, *Red teaming financial crime risks in the banking sector*, „Journal of Financial Crime" 2021, t. 28, nr 1, s. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

[21] *TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym*, Z-LABS, 8 VII 2024 r., https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [dostęp: 19 IV 2025].

[22] *TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [dostęp: 9 II 2026].

rozporządzenie DORA określa, co musi zostać wykonane w ramach testów TLPT, TIBER-EU wskazuje, jak należy to zrobić.

Framework TIBER-EU również zakłada możliwość lokalnej implementacji, żeby lepiej dopasować go do specyfiki danego kraju[23]. Według stanu na kwiecień 2025 r. na implementację zdecydowały się m.in.: Austria, Belgia, Holandia, Francja, Niemcy, Dania, Finlandia, Szwecja i Norwegia.

Dokumentacja TIBER-EU obejmuje liczne opracowania, które mogą być przydatne w trakcie realizacji zarówno testów TLPT, jak i TIBER-EU. Do najważniejszych można zaliczyć:

- *TIBER-EU Guidance for Service Provider Procurement*[24] – zbiór dobrych praktyk w zakresie realizacji procesów zamówień usług red team oraz threat intelligence provider,
- *TIBER-EU Purple-Teaming Guidance*[25] – zbiór dobrych praktyk dotyczących realizacji ćwiczeń purple team, które odbywają się po testach red team,
- *TIBER-EU Scope Specification Document Guidance*[26] – wytyczne odnośnie do odpowiedniego doboru zakresu testów,
- *TIBER-EU Test Summary Report Guidance*[27] – wytyczne na temat opracowania raportu podsumowującego testy.

Główne założenia TIBER-EU to:

- testy oparte na rzeczywistych zagrożeniach (threat intelligence) – scenariusze testowe uwzględniające aktualne informacje o zagrożeniach,
- symulacja rzeczywistych ataków (red teaming) – kontrolowany test, w którym red team symuluje działania cyberprzestępców,
- ochrona krytycznych funkcji – sprawdzenie odporności na ataki dotyczące najważniejszych funkcji biznesowych,

---

[23] *Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce*, Komisja Nadzoru Finansowego, 27 I 2025 r., https://www.knf.gov.pl/?articleId=91971&p_id=18 [dostęp: 19 IV 2025].

[24] *TIBER-EU Guidance for Service Provider Procurement*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [dostęp: 19 IV 2025].

[25] *TIBER-EU Purple Teaming Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee [dostęp: 19 IV 2025].

[26] *TIBER-EU Scope Specification Document Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [dostęp: 19 IV 2025].

[27] *TIBER-EU Test Summary Report Guidance*, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [dostęp: 19 IV 2025].

- współpraca i zgoda – instytucja finansowa dobrowolnie zgadza się na udział w testach,
- standaryzacja i możliwość wdrożenia w różnych krajach UE – model ramowy adaptowany na poziomie krajowym,
- uczenie się i poprawa – faza analizy i nauki (lessons learned) jako istotny element TIBER-EU.

Zespoły realizujące testy TLPT

Jak już wspomniano, testy TLPT cechują się wysoką złożonością. Wymagają różnych kompetencji i umiejętności członków zespołu. Bardzo ważne jest precyzyjne określenie ról, odpowiedzialności i obowiązków zaangażowanych osób i zespołów. Zwiększa to szansę, że każdy aspekt testu będzie dobrze zarządzony, a kolejne działania będą realizowane zgodnie z przyjętym harmonogramem. Precyzyjne zdefiniowanie i przypisanie ról to lepsza koordynacja działań, minimalizacja ryzyka błędów oraz szybkie zidentyfikowanie i odpowiednie zaadresowanie każdego problemu.

Podstawowy model podziału ról, odpowiedzialności i obowiązków zakłada istnienie następujących zespołów:

- TLPT cyber team (TCT),
- control team (CT) znany również jako white team,
- blue team (BT),
- threat intelligence provider (TIP),
- red team (RT),
- purple team (PT).

TLPT cyber team – jest wyznaczany przez uprawniony organ nadzorujący test. Odpowiada za monitorowanie i ocenę prawidłowości przeprowadzania testów, a także ich rzetelne i bezpieczne wykonanie. Powinien zadbać również o to, aby wszystkie aspekty testu były zrealizowane zgodnie z planem, co minimalizuje ryzyko błędów i nieprawidłowości.

Control team (white team) – odgrywa kluczową rolę, gdyż odpowiada za koordynowanie realizacji testów po stronie podmiotu finansowego – planowanie, monitorowanie i zarządzanie ich wszystkimi aspektami. W pracach CT uczestniczą menadżerowie wyższego szczebla i eksperci, którzy dysponują wiedzą na temat infrastruktury oraz procesów operacyjnych organizacji. Zespół odpowiada także za ochronę integralności i stabilności systemów produkcyjnych podczas testowania. Jako jedyny ma informacje na temat szczegółów testów, co pozwala mu na obiektywną ocenę reakcji pracowników organizacji na symulowane zagrożenia.

Blue team – odpowiada za zarządzanie cyberbezpieczeństwem wewnętrznym organizacji i zapewnienie jego odpowiedniego poziomu. Najważniejszym zadaniem tego zespołu jest monitorowanie potencjalnych zagrożeń i reagowanie na nie w czasie rzeczywistym oraz utrzymywanie ochrony systemów i danych przed cyberatakami. Zespół ten nie jest informowany o szczegółach realizowanych testów, co ma pozwolić na przeprowadzenie symulacji w warunkach jak najbardziej zbliżonych do rzeczywistych. Dzięki temu można ocenić reakcje zespołu organizacji na zagrożenia oraz sprawdzić skuteczność istniejących procedur i mechanizmów obronnych, a tym samym lepiej zrozumieć rzeczywisty poziom przygotowania organizacji na incydenty związane z ICT.

Threat intelligence provider – odpowiada za zbieranie informacji o zagrożeniach dotyczących organizacji, przy czym korzysta z metod takich jak OSINT (open source intelligence). Gromadzi dane wywiadowcze, analizuje dostępne źródła publiczne oraz inne źródła informacji, aby stworzyć kompleksowy obraz zagrożeń mogących wpłynąć na organizację. Zespół TIP ma dostarczyć dokładne i aktualne informacje, które pomogą w opracowaniu realistycznych scenariuszy ataków realizowanych przez RT. Dzięki temu testy są lepiej dopasowane do zagrożeń, z jakimi może się zmierzyć organizacja.

Red team – realizuje testy bezpieczeństwa zgodnie z przyjętymi i zaakceptowanymi scenariuszami, wykorzystując informacje, materiały i dane dostarczone przez TIP. Głównym zadaniem RT jest symulowanie rzeczywistych ataków na systemy organizacji, aby ocenić, jak skutecznie potrafią one wykrywać zagrożenia i reagować na nie. Testowane są zarówno zabezpieczenia techniczne, jak i organizacyjne. Holistyczne podejście ma umożliwić identyfikację potencjalnych słabości i luk w zabezpieczeniach organizacji. Red team wykorzystuje różne techniki i metody ataków, aby testy były jak najbardziej realistyczne i skuteczne. Od jakości pracy RT zależy wiarygodność uzyskanych wyników testów. Im ta jakość jest wyższa, tym większa jest szansa na eliminację potencjalnych zagrożeń, mitygację zidentyfikowanych ryzyk oraz wzmocnienie poziomu bezpieczeństwa w kontekście funkcjonowania organizacji.

Purple team – składa się z członków zespołów RT i BT. Zadaniem PT jest analizowanie wyników uzyskanych z testów, identyfikowanie obszarów do poprawy oraz formułowanie rekomendacji, które pomogą wzmocnić zabezpieczenia organizacji. Dzięki współpracy obu zespołów można trafniej ocenić skuteczność istniejących mechanizmów obronnych i zaproponować konkretne działania usprawniające zarówno techniczne, jak i proceduralne aspekty bezpieczeństwa.

Etapy realizacji testów TLPT

Z uwagi na skomplikowaną i wieloaspektową naturę testów TLPT są one realizowane w trzech kolejnych etapach: przygotowanie do testów, ich zrealizowanie i podsumowanie. Podejście to zwiększa szanse przeprowadzenia rzetelnej i pogłębionej oceny odporności organizacji na różne typy zagrożeń.

W etapie pierwszym, czyli przygotowawczym, są przeprowadzane następujące działania:

- spotkania wstępne podmiotu realizującego testy z organem nadzorującym i zespołem TCT, aby omówić i uzgodnić szczegóły dotyczące testów, w tym cele, metodologię oraz kryteria oceny;
- określenie zakresu testu, tj. obszarów do testowania oraz potencjalnych zagrożeń, które mają zostać uwzględnione. W tym kroku również są ustalane cele testu, a także oczekiwane wyniki;
- procesy zakupowe, aby wyłonić odpowiednie zespoły RT oraz TIP. Wybór tych zespołów ma decydujące znaczenie dla zapewnienia wysokiej jakości testów i realistycznych scenariuszy ataków;
- przygotowanie dokumentacji, w której są określone wszystkie aspekty testów, w tym harmonogram, zasady komunikacji oraz procedury bezpieczeństwa. Dokumentacja ta stanowi podstawę dla kolejnych etapów testowania i potwierdza, że wszystkie strony są zgodne co do oczekiwań i obowiązków.

Etap drugi, w ramach którego są realizowane główne działania testowe, obejmuje:

- opracowanie raportu TTI (targeted threat intelligence) i scenariuszy ataku – zespół TIP przygotowuje raport dotyczący ukierunkowanych zagrożeń TTI oraz wstępne scenariusze ataku. Raport ten zawiera szczegółowe informacje na temat potencjalnych zagrożeń oraz wektorów ataków mogących wpływać na organizację. Na tej podstawie zespół TIP tworzy realistyczne scenariusze ataków, które będą wykorzystywane w dalszej części testowania;
- przeprowadzenie testów przez RT z uwzględnieniem scenariuszy opracowanych przez zespół TIP, co pozwala na dokładną ocenę odporności systemów i procedur organizacji. Red team wykorzystuje różne techniki i metody ataków, aby sprawdzić, jak skutecznie organizacja radzi sobie z zagrożeniami.

Etap trzeci to podsumowanie i analiza uzyskanych wyników testów, a także opracowanie rekomendacji. Składa się na to:

- opracowanie raportów przez zespoły RT i BT. Zawierają one analizy wyników, opis przeprowadzonych scenariuszy ataku oraz ocenę efektywności reakcji i obrony. Dokumenty te są podstawą do dalszej analizy i wniosków dotyczących bezpieczeństwa organizacji;
- przeprowadzenie warsztatów purple teaming, w ramach których zespoły RT i BT omawiają zrealizowane scenariusze ataku, aby wymienić między sobą informacje i doświadczenia. Pozwala to na lepsze zrozumienie skuteczności testów oraz identyfikację obszarów do poprawy, jak również pomaga w opracowaniu praktycznych rekomendacji oraz planów usprawnień;
- przygotowanie końcowego raportu z realizacji testów TLPT na podstawie raportów zespołów RT i BT oraz wyników warsztatów. Obejmuje on podsumowanie całokształtu przeprowadzonych działań, wnioski z testów oraz zalecenia dotyczące poprawy zabezpieczeń. Dokument jest przekazywany organizacji i stanowi podstawę do wdrażania zmian w zakresie bezpieczeństwa.

Podsumowanie i wnioski

Jak wykazano w artykule, podstawowym założeniem testów TLPT jest jak najwierniejsze odwzorowanie rzeczywistych ataków. Umożliwia to sprawdzenie nie tylko efektywności zabezpieczeń systemów informatycznych, lecz także poziomu bezpieczeństwa procesów operacyjnych i świadomości pracowników w zakresie cyberzagrożeń, co zwiększa precyzję oceny odporności systemów i procedur organizacji. Ze względu na złożoność i różnorodność testów TLPT ich wdrożenie może jednak stanowić wyzwanie dla organizacji. Wymagają one starannego przygotowania i odpowiednich procedur, które zapewnią zarówno skuteczność testów, jak i bezpieczeństwo organizacji podczas ich realizacji.

Analiza przeprowadzona na potrzeby artykułu prowadzi do wniosku, że wdrożenie testów TLPT jako standardu dla podmiotów finansowych było krokiem w dobrym kierunku. Nie ulega bowiem wątpliwości, że w złożonym środowisku cyfrowym konieczne jest rozwijanie skutecznych mechanizmów zarządzania ryzykiem opartych na rzeczywistych czynnikach i wyzwaniach, a nie wyłącznie tych definiowanych na potrzeby budowania odpowiednich modeli. Autorzy podzielają stanowisko Europejskiego Banku Centralnego, który podkreśla, że testy TLPT pozwalają na weryfikowanie nie tylko środków technicznych, lecz także personelu i procesów. Bank ten słusznie zwraca uwagę, że (…) *wyniki tych testów mogą znacząco podnieść świadomość bezpieczeństwa wśród kadry kierowniczej wyższego*

szczebla testowanych podmiotów[28]. Rację ma także Wojciech Dworakowski, wskazując, że TLPT to inwestycja w bezpieczeństwo, która się zwraca, ponieważ lepiej działać proaktywnie, niż naprawiać skutki cyberataku[29].

W perspektywie kolejnych lat kluczowe będzie zapewnienie konsekwentnego i proporcjonalnego stosowania testów TLPT w całym sektorze finansowym UE. Nadzór finansowy powinien tę możliwość wykorzystywać, wspierając podmioty w przygotowaniu do tych testów oraz w rozwijaniu zdolności obrony przed cyberatakami. Weryfikacja odporności organizacji za pomocą realistycznych scenariuszy ataków powinna istotnie przyczynić się do poprawy cyberodporności całego rynku finansowego.

Bibliografia

Bayle de Jessé M., *The Eurosystem's cyber resilience strategy for financial market infrastructures*, „Cyber Security: A Peer-Reviewed Journal" 2019, t. 2, nr 4, s. 294–302. https://doi.org/10.69554/DFBJ2963.

Cichocki C., Komentarz do art. 26, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 276–282.

Cichocki C., Komentarz do art. 27, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 283–286.

Dozsa M.L., *Modular Automated Cyber Range Deployment with Adversary Emulation. In Compliance with the Digital Operational Resilience Act (DORA)*, praca magisterska, Oslo 2024.

Kurek-Sobieraj J., Komentarz do art. 3, w: *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, J. Byrski, J. Kurek-Sobieraj (red.), Warszawa 2025, s. 69–106.

[28] *Opinia Europejskiego Banku Centralnego z dnia 4 czerwca 2021 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (CON/2021/20)*, s. 1.

[29] W. Dworakowski, *Threat-Led Penetration Testing (TLPT) – Jak być zgodnym z DORA w 2025 roku?*, Securing, 28 II 2025 r., https://www.securing.pl/pl/threat-led-penetration-testing-tlpt-jak-byc-zgodnym-z-dora-w-2025-roku-2/#Czym-s%C4%85-testy-TLPT-i-dlaczego-s%C4%85-kluczowe-dla-DORA [dostęp: 18 IV 2025].

Riaz B., Younas Z., *Investigating the impact of DORA Regulations on Third Party Risk Management in the Swedish Financial Sector*, Stockholm University 2024.

Scott B.F., *Red teaming financial crime risks in the banking sector*, „Journal of Financial Crime" 2021, t. 28, nr 1, s. 98–111. https://doi.org/10.1108/JFC-06-2020-0118.

Valkeasuo T., *TIBER-EU Preparation Phase Framework. Case study Nixu: optimizing TIBER-EU engagements*, Jyväskylä: JAMK University of Applied Sciences, March 2023.

Źródła internetowe

Dworakowski W., *Threat-Led Penetration Testing (TLPT) – Jak być zgodnym z DORA w 2025 roku?*, Securing, 28 II 2025 r., https://www.securing.pl/pl/threat-led-penetration-testing-tlpt-jak-byc-zgodnym-z-dora-w-2025-roku-2/#Czym-s%C4%85-testy-TLPT-i-dlaczego-s%C4%85-kluczowe-dla-DORA [dostęp: 18 IV 2025].

Implementacje frameworku TIBER-EU w Europie a wdrożenie w Polsce, Komisja Nadzoru Finansowego, 27 I 2025 r., https://www.knf.gov.pl/?articleId=91971&p_id=18 [dostęp: 19 IV 2025].

Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025, CSIRT KNF, https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf [dostęp: 19 I 2026].

Testy TLPT – cyfrowa odporność organizacji zgodnie z rozporządzeniem DORA, Bankowe ABC, 2 I 2025 r., https://bankoweabc.pl/2025/01/02/testy-tlpt-a-dora/ [dostęp: 19 IV 2025].

Testy TLPT – nowe podejście do testowania cyfrowej odporności organizacji, Komisja Nadzoru Finansowego, 14 VII 2025 r., https://www.knf.gov.pl/dla_rynku/dora/wymagania_rozporzadzenia_dora/testy_TLPT_nowe_podejscie?articleId=90547&p_id=18 [dostęp: 9 II 2026].

TIBER-EU Framework. How to implement the European framework for Threat Intelligence-Based Ethical Red teaming, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.pl.pdf?0309990e5e167a47ca4748370a949064 [dostęp: 9 II 2026].

TIBER-EU Guidance for Service Provider Procurement, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_service_provider_procurement_2025.en.pdf?1d229f2191835b83770d593a44f69b14 [dostęp: 19 IV 2025].

TIBER-EU i DORA szansą na budowanie realnej cyberodporności w sektorze finansowym, Z-LABS, 8 VII 2024 r., https://blog.z-labs.eu/2024/07/08/tiber-eu-dora-cyberodpornosc.html [dostęp: 19 IV 2025].

TIBER-EU Purple Teaming Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff-75caf6e644af0fd757415aee [dostęp: 19 IV 2025].

TIBER-EU Scope Specification Document Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_scope_specification_document_guidance_2025.en.pdf?67dc9f94d617ea2522e9a3764f43b92c [dostęp: 19 IV 2025].

TIBER-EU Test Summary Report Guidance, European Central Bank, January 2025, https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_test_summary_report_guidance_2025.en.pdf?ecc819840c37a008b908578dd1d48b50 [dostęp: 19 IV 2025].

Ustawa wdrażająca DORA do prawa polskiego, „Biuletyn prawny dla branży finansowej", Deloitte, https://www.deloitte.com/pl/pl/Industries/financial-services/perspectives/ustawa-wdrazajaca-DORA-do-prawa-polskiego.html [dostęp: 12 IV 2025].

Akty prawne

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 (Dz. Urz. UE L 333 z 2022 r., ze zm.).

Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz. Urz. UE L 287 z 2013 r.).

Ustawa z dnia 25 czerwca 2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (DzU z 2025 r. poz. 1069).

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. DzU z 2025 r. poz. 640, ze zm.).

Inne dokumenty

Final Report. Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554, European Banking Authority, 17 July 2024.

Opinia Europejskiego Banku Centralnego z dnia 4 czerwca 2021 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (CON/2021/20) – (Dz. Urz. UE C 343/1 z 2021 r.).

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji, druk nr UC11, Rządowe Centrum Legislacji, Warszawa 2025.

Dr hab. Kamil Mroczka

Doktor habilitowany nauk społecznych w zakresie nauk o polityce i administracji, adiunkt w Katedrze Nauk o Państwie i Administracji Publicznej Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego, absolwent programu Executive MBA. Ma wieloletnie doświadczenie na stanowiskach kierowniczych w administracji publicznej oraz w sektorze prywatnym. Obecnie zatrudniony jako Chief Compliance Officer w Santander Bank Polska.

Kontakt: ks.mroczka@uw.edu.pl

Paweł Piekutowski

Absolwent Wojskowej Akademii Technicznej. Ma wieloletnie doświadczenie w zakresie cyberbezpieczeństwa, zwłaszcza w obszarze testów penetracyjnych. Obecnie pełni funkcję zastępcy dyrektora Departamentu Cyberbezpieczeństwa w Urzędzie Komisji Nadzoru Finansowego.

Kontakt: pawel.piekutowski@gmail.com