					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P40					Tytuł dokumentu: **Polityka testów bezpieczeństwa i ćwiczeń Red Team**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
RODO	Art. 32(1)(d)	
Dyrektywa NIS2	Art. 21(2)(f)	
Rozporządzenie DORA	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Cel

1 Celem niniejszej polityki jest ustanowienie ustrukturyzowanego programu regularnych testów bezpieczeństwa sieci, systemów i aplikacji organizacji, w tym ocen podatności, testów penetracyjnych oraz ćwiczeń Red Team, w celu spełnienia wymagań art. 21 ust. 2 lit. f dyrektywy NIS2 dotyczących oceny skuteczności środków cyberbezpieczeństwa.

1.1 Organizacja musi zapewnić proaktywną identyfikację i usuwanie słabości w środkach technicznych i organizacyjnych poprzez kontrolowane testy, tak aby stale doskonalić swój profil ryzyka w obszarze bezpieczeństwa.

2. Zakres

2 Niniejsza polityka obejmuje wszystkie krytyczne systemy informatyczne, aplikacje oraz infrastrukturę wspierającą będące własnością organizacji lub przez nią eksploatowane. Obejmuje również testy bezpieczeństwa fizycznego obiektów w zakresie istotnym z punktu widzenia cyberbezpieczeństwa, na przykład testy socjotechniczne lub fizyczne testy penetracyjne, jeżeli mieszczą się one w zakresie ćwiczeń Red Team.

2.1 Polityka ma zastosowanie do wewnętrznych zespołów bezpieczeństwa, wszelkich zakontraktowanych podmiotów zewnętrznych realizujących testy bezpieczeństwa oraz odpowiednich właścicieli systemów i właścicieli aplikacji. Wszystkie działania testowe muszą być autoryzowane i realizowane zgodnie z niniejszymi procedurami, aby uniknąć niezamierzonych zakłóceń.

3. Cele

3 Organizacja musi weryfikować skuteczność wdrożonych zabezpieczeń cyberbezpieczeństwa, technicznych, operacyjnych i organizacyjnych, poprzez okresowe testy i symulacje, zgodnie z wymogiem dyrektywy NIS2 dotyczącym pomiaru skuteczności.

3.1 Organizacja musi wykrywać podatności lub luki, które mogą zostać pominięte przez standardowe procesy operacyjne, w tym podatności typu zero-day lub błędy konfiguracji, w realistycznych scenariuszach ataku w ramach ćwiczeń Red Team, zanim zostaną wykorzystane przez aktora zagrożenia.

3.2 Organizacja musi dostarczać kierownictwu zapewnienie oraz praktyczne rekomendacje poprzez raportowanie wyników testów, umożliwiając tym samym podejmowanie świadomych decyzji dotyczących postępowania z ryzykiem oraz ciągłe doskonalenie programu bezpieczeństwa.

4. Role i obowiązki

4 Koordynator Testów Bezpieczeństwa (STC): wyznaczany przez Dyrektora ds. Bezpieczeństwa Informacji (CISO), odpowiedzialny za planowanie i nadzór nad wszystkimi działaniami w zakresie testów bezpieczeństwa. Zapewnia określenie zakresu testów, ich autoryzację, raportowanie wyników oraz realizację działań następczych.

4.1 Wewnętrzny zespół bezpieczeństwa (Blue Team): współpracuje przy testach, na przykład dostarcza informacje na potrzeby określenia zakresu oraz monitoruje systemy w trakcie testów. W przypadku ćwiczeń Red Team Blue Team reaguje na symulowane ataki, a jego zdolności wykrywania i reagowania podlegają ocenie.

4.2 Red Team / testerzy penetracyjni: mogą stanowić wewnętrzny zespół bezpieczeństwa ofensywnego lub zewnętrznych konsultantów. Realizują testy zgodnie z uzgodnionymi zasadami prowadzenia działań, dokumentują wszystkie wykryte podatności i ścieżki eksploatacji oraz zachowują poufność.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Monitorowanie i audyt

9 STC prowadzi kalendarz i rejestr wszystkich zrealizowanych działań testowych w zakresie bezpieczeństwa. Rejestr ten powinien obejmować datę, zakres, wykonawcę testu oraz podsumowanie wyników. Podlega on przeglądowi w celu zapewnienia zgodności z wymaganym harmonogramem, na przykład aby żaden system krytyczny nie pozostawał bez testów dłużej niż przez jeden rok.

9.1 Postęp działań naprawczych dotyczących ustaleń z testów musi być monitorowany i raportowany co miesiąc. Otwarte kwestie o wysokiej wadze muszą być omawiane na spotkaniach kierownictwa aż do ich zamknięcia.

9.2 Funkcja audytu wewnętrznego / zgodności lub niezależny audytor dokonuje corocznego przeglądu programu testów bezpieczeństwa w celu weryfikacji, że testy są prawidłowo autoryzowane, prowadzone i raportowane, ustalenia krytyczne zostały zaadresowane, a program spełnia oczekiwania regulacyjne. Przykładowo audytorzy mogą sprawdzić, czy test penetracyjny został wykonany przed uruchomieniem nowej usługi online, jeżeli jest to wymagane. Wszelkie odstępstwa skutkują planami działań korygujących.

10. Przegląd i utrzymanie

10 Niniejsza polityka oraz ogólny plan testów podlegają przeglądowi co najmniej raz w roku. Przegląd uwzględnia zmiany w krajobrazie zagrożeń, na przykład pojawienie się nowych technik ataku, których obecne testy mogą nie obejmować, i odpowiednio dostosowuje zakresy lub częstotliwości.

10.1 Po każdym istotnym incydencie cyberbezpieczeństwa lub naruszeniu bezpieczeństwa niniejsza polityka musi zostać ponownie przeanalizowana w celu ustalenia, czy dodatkowe lub częstsze testy mogłyby zapobiec problemowi lub umożliwić jego wykrycie. Następnie polityka musi zostać zaktualizowana z uwzględnieniem takich zmian, na przykład przez dodanie nowego scenariusza do ćwiczeń Red Team na podstawie zaobserwowanych wzorców ataku.

10.2 Aktualizacje niniejszej polityki muszą być zatwierdzane przez Dyrektora ds. Bezpieczeństwa Informacji (CISO) i odnotowywane przez zarząd. Cały odpowiedni personel musi zostać poinformowany o zmianach, a zewnętrzni partnerzy testowi muszą zostać powiadomieni, jeżeli jakakolwiek zmiana wpływa na warunki współpracy.

11. Powiązane polityki i zależności

11.1 P06 – Polityka zarządzania ryzykiem. Wyniki testów stanowią podstawę oceny ryzyka i postępowania z ryzykiem.

11.2 P22 – Polityka logowania i monitorowania. Umożliwia walidację pokrycia wykrywania podczas ćwiczeń.

11.3 P24 – Polityka bezpiecznego rozwoju oprogramowania. Integruje ustalenia z testów ze środkami kontrolnymi w cyklu życia rozwoju oprogramowania (SDLC).

11.4 P25 – Polityka wymagań bezpieczeństwa aplikacji. Zapewnia odzwierciedlenie wniosków z testów w wymaganiach.

11.5 P30 – Polityka reagowania na incydenty. Scenariusze Red Team doskonalą procedury reagowania na incydenty i samo reagowanie.

11.6 P31 – Polityka zabezpieczania materiału dowodowego i informatyki śledczej. Umożliwia bezpieczne gromadzenie artefaktów podczas testów.

11.7 P32 – Polityka ciągłości działania i odtwarzania po awarii. Ćwiczenia weryfikują odporność na atak.

11.8 P33 – Polityka audytu i monitorowania zgodności. Zapewnia niezależny nadzór nad skutecznością programu testowego.

12. Odniesienia

12.1 Dyrektywa NIS2 (UE 2022/2555), art. 21 ust. 2 lit. f (polityki i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa)

12.2 Rozporządzenie wykonawcze Komisji (UE) 2024/2690, załącznik, sekcja 7 (wymagania dotyczące monitorowania, testowania i oceny skuteczności środków cyberbezpieczeństwa)

12.3 Wytyczne techniczne ENISA (2025) – załącznik dotyczący testów bezpieczeństwa i audytu (wytyczne dotyczące prowadzenia ćwiczeń cyberbezpieczeństwa i testów technicznych)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Dobre praktyki branżowe: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (ramy ćwiczeń Red Team dla sektora finansowego, jako materiał odniesienia)