					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P40					Název dokumentu: **Politika bezpečnostního testování a cvičení Red Teamu**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
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	
GDPR	čl. 32 odst. 1 písm. d)	
směrnice NIS2	čl. 21 odst. 2 písm. f)	
nařízení DORA	čl. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Účel

1 Stanovit strukturovaný program pravidelného bezpečnostního testování sítí, systémů a aplikací organizace, včetně hodnocení zranitelností, penetračního testování a cvičení Red Teamu, za účelem splnění požadavků čl. 21 odst. 2 písm. f) směrnice NIS2 na posuzování účinnosti opatření kybernetické bezpečnosti.

1.1 Zajistit, aby byly slabiny v technických a organizačních opatřeních proaktivně identifikovány a odstraněny prostřednictvím řízeného testování, a tím průběžně zlepšován stav bezpečnosti organizace.

2. Rozsah

2 Tato politika se vztahuje na všechny kritické informační systémy, aplikace a podpůrnou infrastrukturu vlastněné nebo provozované organizací. Zahrnuje rovněž testování fyzické bezpečnosti objektů v rozsahu relevantním pro kybernetickou bezpečnost (např. sociální inženýrství nebo fyzické penetrační testy, pokud jsou součástí rozsahu cvičení Red Teamu).

2.1 Tato politika se vztahuje na interní bezpečnostní týmy, smluvně zajištěné externí společnosti provádějící bezpečnostní testování a příslušné vlastníky systémů a aplikací. Veškeré testovací činnosti musí být schváleny a prováděny v souladu s tímto dokumentem, aby nedošlo k neúmyslnému narušení provozu.

3. Cíle

3 Ověřovat účinnost zavedených opatření kybernetické bezpečnosti (technických, provozních a organizačních) prostřednictvím pravidelného testování a simulací v souladu s požadavkem směrnice NIS2 na měření účinnosti.

3.1 Odhalovat zranitelnosti nebo mezery, které mohou běžné provozní procesy přehlédnout, včetně zero-day zranitelností nebo chybných konfigurací, v realistických scénářích útoku (cvičení Red Teamu) dříve, než je protivník zneužije.

3.2 Poskytovat vedení ujištění a realizovatelná doporučení prostřednictvím vykazování zjištění z testování, a tím umožnit informovaná rozhodnutí o ošetření rizik a neustálé zlepšování bezpečnostního programu.

4. Role a odpovědnosti

4 Koordinátor bezpečnostního testování (STC): Jmenován CISO, odpovídá za plánování a dohled nad všemi činnostmi bezpečnostního testování. Zajišťuje vymezení rozsahu testů, jejich schválení a vykazování výsledků včetně následných opatření.

4.1 Interní bezpečnostní tým (Blue Team): Spolupracuje při testech (např. poskytuje informace pro vymezení rozsahu a monitoruje systémy během testů). Při cvičeních Red Teamu Blue Team reaguje na simulované útoky a jsou hodnoceny jeho schopnosti detekce a reakce.

4.2 Red Team / penetrační testeři: Mohou být interním ofenzivním bezpečnostním týmem nebo externími konzultanty. Provádějí testy podle schválených pravidel zapojení, dokumentují všechny zjištěné zranitelnosti a cesty zneužití a zachovávají důvěrnost informací.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Monitorování a audit

9 STC vede kalendář a evidenci všech provedených činností bezpečnostního testování. Tato evidence musí obsahovat datum, rozsah, kdo test provedl a souhrn výsledků. Bude přezkoumávána za účelem ověření dodržování požadovaného harmonogramu (např. aby žádný kritický systém nezůstal netestován déle než jeden rok).

9.1 Postup nápravy zjištění z testování bude monitorován a měsíčně vykazován. Neuzavřené problémy s vysokou závažností budou přezkoumávány na jednáních vedení až do jejich uzavření.

9.2 Interní audit nebo nezávislý auditor každoročně přezkoumá program bezpečnostního testování a ověří, že: testy jsou řádně schváleny, provedeny a vykázány; kritická zjištění byla řešena; a program splňuje regulační očekávání (auditoři mohou například ověřit, že před spuštěním nové online služby bylo provedeno penetrační testování, pokud to bylo vyžadováno). Jakékoli odchylky povedou k plánům nápravných opatření.

10. Přezkum a údržba

10 Tato politika a celkový plán testování musí být přezkoumávány nejméně jednou ročně. Při přezkumu se zohlední změny v prostředí hrozeb (např. vznik nových technik útoku, které současné testování nepokrývá) a podle toho se upraví rozsah nebo četnost testování.

10.1 Po každém závažném kybernetickém incidentu nebo porušení zabezpečení dat musí být tato politika znovu posouzena s cílem určit, zda by dodatečné nebo častější testování mohlo problému předejít nebo jej odhalit. Politika bude následně aktualizována tak, aby takové úpravy zohlednila (například doplněním nového scénáře do cvičení Red Teamu na základě pozorovaných vzorců útoku).

10.2 Aktualizace této politiky musí schválit CISO a správní rada je musí vzít na vědomí. Veškerý relevantní personál bude o změnách informován a externí testovací partneři budou vyrozuměni, pokud jakákoli změna ovlivní podmínky jejich zapojení.

11. Související politiky a vazby

11.1 P06 – Politika řízení rizik. Výstupy z testování jsou vstupem pro vyhodnocení rizik a jejich ošetření.

11.2 P22 – Politika protokolování a monitorování. Ověřuje pokrytí detekce během cvičení.

11.3 P24 – Politika bezpečného vývoje. Začleňuje zjištění z testování do opatření SDLC.

11.4 P25 – Politika požadavků na zabezpečení aplikací. Zajišťuje, aby požadavky odrážely poznatky z testování.

11.5 P30 – Politika reakce na incidenty. Scénáře Red Teamu zpřesňují playbooky a reakci.

11.6 P31 – Politika sběru důkazů a forenzního šetření. Zajišťuje bezpečný sběr artefaktů během testování.

11.7 P32 – Politika kontinuity činností a obnovy po havárii. Cvičení ověřují odolnost při útoku.

11.8 P33 – Politika monitorování auditu a souladu. Zajišťuje nezávislý dohled nad účinností programu testování.

12. Reference

12.1 Směrnice NIS2 (EU 2022/2555), čl. 21 odst. 2 písm. f) (politiky a postupy pro posuzování účinnosti opatření řízení rizik kybernetické bezpečnosti)

12.2 Prováděcí nařízení Komise (EU) 2024/2690, příloha, oddíl 7 (požadavky na monitorování, testování a vyhodnocování účinnosti opatření kybernetické bezpečnosti)

12.3 Technické pokyny ENISA (2025) – příloha k bezpečnostnímu testování a auditu (pokyny pro provádění cvičení kybernetické bezpečnosti a technických testů)

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

12.5 Osvědčené postupy v odvětví: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (rámce red teamingu ve finančním sektoru pro referenci)