					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P40					Názov dokumentu: **Politika bezpečnostného testovania a cvičení red teamu**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
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 EÚ	Čl. 32 ods. 1 písm. d)	
Smernica EÚ NIS2	Čl. 21 ods. 2 písm. f)	
Nariadenie EÚ DORA	Čl. 25 – 27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Účel

1 Zaviesť štruktúrovaný program pravidelného bezpečnostného testovania sietí, systémov a aplikácií organizácie vrátane posudzovania zraniteľností, penetračného testovania a cvičení red teamu s cieľom splniť požiadavky článku 21 ods. 2 písm. f) smernice EÚ NIS2 na posudzovanie účinnosti opatrení kybernetickej bezpečnosti.

1.1 Zabezpečiť, aby sa slabé miesta v technických a organizačných opatreniach proaktívne identifikovali a odstraňovali prostredníctvom riadeného testovania, a tým sa priebežne zlepšovala úroveň bezpečnosti organizácie.

2. Rozsah

2 Táto politika sa vzťahuje na všetky kritické informačné systémy, aplikácie a podpornú infraštruktúru vo vlastníctve organizácie alebo prevádzkované organizáciou. Zahŕňa aj testovanie fyzickej bezpečnosti priestorov v rozsahu relevantnom pre kybernetickú bezpečnosť, napríklad sociálne inžinierstvo alebo fyzické penetračné testy, ak sú súčasťou rozsahu cvičení red teamu.

2.1 Politika sa vzťahuje na interné bezpečnostné tímy, všetky zmluvne zabezpečené externé spoločnosti poskytujúce bezpečnostné testovanie a príslušných vlastníkov systémov a aplikácií. Všetky testovacie činnosti musia byť autorizované a vykonávané v súlade s touto politikou, aby sa predišlo neúmyselným prevádzkovým narušeniam.

3. Ciele

3 Overovať účinnosť zavedených kontrol kybernetickej bezpečnosti (technických, prevádzkových a organizačných) prostredníctvom pravidelného testovania a simulácií v súlade s požiadavkou smernice EÚ NIS2 na meranie účinnosti.

3.1 Identifikovať zraniteľnosti alebo medzery, ktoré môžu bežné prevádzkové procesy prehliadnuť, vrátane zero-day zraniteľností alebo chýb konfigurácie, a to v realistických scenároch útoku v rámci cvičení red teamu ešte predtým, ako ich zneužije pôvodca hrozby.

3.2 Poskytovať vedeniu uistenie a realizovateľné odporúčania prostredníctvom správ o výsledkoch testovania, čím sa umožní informované ošetrenie rizík a nepretržité zlepšovanie bezpečnostného programu.

4. Roly a zodpovednosti

4 Koordinátor bezpečnostného testovania (STC): určuje ho riaditeľ informačnej bezpečnosti (CISO) a zodpovedá za plánovanie a dohľad nad všetkými činnosťami bezpečnostného testovania.

Zabezpečuje definovanie rozsahu testov, ich autorizáciu, ako aj vykazovanie výsledkov a prijímanie nadväzných opatrení.

4.1 Interný bezpečnostný tím (Blue Team): spolupracuje pri testoch, napríklad poskytuje informácie na určenie rozsahu a monitoruje systémy počas testovania. Pri cvičeniach red teamu Blue Team reaguje na simulované útoky a vyhodnocuje sa jeho schopnosť detekcie a reakcie.

4.2 Red Team / penetrační testeri: môže ísť o interný tím ofenzívnej bezpečnosti alebo externých konzultantov. Vykonávajú testy podľa dohodnutých pravidiel realizácie, dokumentujú všetky zistené zraniteľnosti a cesty zneužitia a zachovávajú dôvernosť informácií.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Monitorovanie a audit

9 STC vedie kalendár a záznam o všetkých vykonaných činnostiach bezpečnostného testovania. Tento záznam musí obsahovať dátum, rozsah, vykonávateľa testu a súhrn výsledkov. Záznam sa preskúmava s cieľom overiť dodržiavanie požadovaného harmonogramu, napríklad aby žiadny kritický systém nezostal bez testovania dlhšie ako jeden ročný cyklus.

9.1 Pokrok pri náprave zistení z testovania sa monitoruje a vykazuje mesačne. Otvorené problémy s vysokou závažnosťou sa preskúmavajú na stretnutiach manažmentu až do ich uzatvorenia.

9.2 Tím vnútorného auditu alebo nezávislý audítor preskúma program bezpečnostného testovania najmenej raz ročne s cieľom overiť, že testy sú riadne autorizované, vykonané a vykázané, že kritické zistenia boli riešené a že program spĺňa regulačné očakávania. Audítori môžu napríklad overovať, že penetračný test bol vykonaný pred spustením novej online služby, ak sa to vyžaduje. Každá odchýlka vedie k vypracovaniu plánu nápravy.

10. Preskúmanie a údržba

10 Táto politika a celkový plán testovania sa musia preskúmať najmenej raz ročne. Pri preskúmaní sa zohľadnia zmeny v prostredí hrozieb, napríklad vznik nových techník útokov, ktoré súčasné testovanie nepokrýva, a podľa toho sa upraví rozsah alebo frekvencia testovania.

10.1 Po každom významnom incidente kybernetickej bezpečnosti alebo porušení ochrany údajov sa táto politika musí opätovne posúdiť s cieľom určiť, či by dodatočné alebo častejšie testovanie mohlo problému predísť alebo ho odhaliť. Politika sa následne aktualizuje tak, aby tieto úpravy zohľadnila, napríklad doplnením nového scenára do cvičení red teamu na základe pozorovaných vzorcov útokov.

10.2 Aktualizácie tejto politiky musí schváliť CISO a predstavenstvo ich musí vziať na vedomie. O všetkých zmenách musia byť informované všetky relevantné osoby a externí partneri zabezpečujúci testovanie musia byť upovedomení, ak zmena ovplyvňuje podmienky ich spolupráce.

11. Súvisiace politiky a väzby

11.1 P06 – Politika riadenia rizík. Výstupy z testovania sú vstupom do hodnotenia a ošetrenia rizík.

11.2 P22 – Politika logovania a monitorovania. Overuje pokrytie detekcie počas cvičení.

11.3 P24 – Politika bezpečného vývoja. Integruje zistenia z testovania do kontrol SDLC.

11.4 P25 – Politika požiadaviek na bezpečnosť aplikácií. Zabezpečuje, aby požiadavky zohľadňovali poznatky z testovania.

11.5 P30 – Politika reakcie na incidenty. Scenáre red teamu spresňujú playbooky a reakciu.

11.6 P31 – Politika zberu dôkazov a forenznej analýzy. Počas testovania bezpečne zhromažďuje artefakty.

11.7 P32 – Politika kontinuity činností a obnovy po havárii. Cvičenia overujú odolnosť pri útoku.

11.8 P33 – Politika monitorovania auditov a súladu. Zabezpečuje nezávislý dohľad nad účinnosťou programu testovania.

12. Referencie

12.1 Smernica NIS2 (EÚ 2022/2555), článok 21 ods. 2 písm. f) (politiky a postupy na posudzovanie účinnosti opatrení riadenia rizík kybernetickej bezpečnosti)

12.2 Vykonávacie nariadenie Komisie (EÚ) 2024/2690, príloha, oddiel 7 (požiadavky na monitorovanie, testovanie a hodnotenie účinnosti opatrení kybernetickej bezpečnosti)

12.3 Technické usmernenie ENISA (2025) – príloha o bezpečnostnom testovaní a audite (usmernenia na vykonávanie cvičení kybernetickej bezpečnosti a technických testov)

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

12.5 Odvetvové osvedčené postupy: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (rámce red teamu vo finančnom sektore na referenčné účely)