					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P40					Dokumento pavadinimas: **Saugumo testavimo ir „Red Team“ pratybų politika**						
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:						
X	Politika		Standartas		Procedūra		Forma		Registras		Kita

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Punktas / straipsnis	Komentaras
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	
ES BDAR	32 str. 1 d. d punktas	
ES NIS2 direktyva	21 str. 2 d. f punktas	
ES DORA reglamentas	25–27 str.	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Tikslas

1 Apibrėžti struktūrizuotą reguliaraus organizacijos tinklų, sistemų ir taikomųjų programų saugumo testavimo programą, įskaitant pažeidžiamumų vertinimą, įsiskverbimo testavimą ir „Red Team“ pratybas, siekiant įvykdyti ES NIS2 direktyvos 21 straipsnio 2 dalies f punkto reikalavimus dėl kibernetinio saugumo priemonių veiksmingumo vertinimo.

1.1 Užtikrinti, kad techninių ir organizacinių priemonių trūkumai būtų aktyviai nustatomi ir šalinami atliekant kontroliuojamą testavimą, taip nuolat gerinant organizacijos saugumo būklę.

2. Taikymo sritis

2 Ši politika taikoma visoms organizacijai priklausančioms arba jos valdomoms kritinėms informacinėms sistemoms, taikomosioms programoms ir jas palaikančiai infrastruktūrai. Ji taip pat apima objektų fizinio saugumo testavimą tiek, kiek tai susiję su kibernetiniu saugumu, pavyzdžiui, socialinės inžinerijos ar fizinio įsiskverbimo testus, jei jie įtraukti į „Red Team“ pratybų taikymo sritį.

2.1 Politika taikoma vidaus saugumo komandoms, visoms pasitelktoms išorės saugumo testavimo įmonėms ir atitinkamiems sistemų bei taikomųjų programų savininkams. Visa testavimo veikla turi būti autorizuota ir vykdoma pagal šioje politikoje nustatytas procedūras, siekiant išvengti nenumatytų veiklos sutrikimų.

3. Tikslai

3 Patvirtinti įdiegtų kibernetinio saugumo kontrolės priemonių (techninių, veiklos ir organizacinių) veiksmingumą vykdant periodinį testavimą ir simuliacijas, laikantis ES NIS2 direktyvos reikalavimo vertinti veiksmingumą.

3.1 Nustatyti pažeidžiamumus ar spragas, kurių įprasti veiklos procesai gali neaptikti, įskaitant nulinės dienos pažeidžiamumus ar konfigūracijos klaidas, taikant realistiškus atakų scenarijus („Red Team“), prieš jais pasinaudojant grėsmės veikėjams.

3.2 Teikti vadovybei užtikrinimą ir įgyvendinamas rekomendacijas, pateikiant testavimo išvadas, taip sudarant sąlygas priimti pagrįstus sprendimus dėl rizikos valdymo ir nuolatinio saugumo programos tobulinimo.

4. Vaidmenys ir atsakomybės

4 Saugumo testavimo koordinatorius (STC): skiriamas vyriausiojo informacijos saugumo pareigūno, atsako už visų saugumo testavimo veiklų planavimą ir priežiūrą. Užtikrina, kad testams

būtų apibrėžta taikymo sritis, suteiktas autorizavimas, o rezultatai būtų pateikti ir pagal juos būtų imamasi veiksmų.

4.1 Vidaus saugumo komanda („Blue Team“): bendradarbiauja vykdant testus, pavyzdžiui, teikia informaciją taikymo sričiai nustatyti ir stebi sistemas testų metu. „Red Team“ pratybų metu „Blue Team“ reaguoja į simuliuojamas atakas, o jos aptikimo ir reagavimo gebėjimai yra vertinami.

4.2 „Red Team“ / įsiskverbimo testuotojai: tai gali būti vidaus puolamojo saugumo komanda arba išorės konsultantai. Jie vykdo testus pagal sutartas veiklos taisykles, dokumentuoja visus nustatytus pažeidžiamumus ir išnaudojimo grandines bei užtikrina konfidencialumą.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Stebėsena ir auditas

9 Saugumo testavimo koordinatorius turi tvarkyti visų atliktų saugumo testavimo veiklų kalendorių ir žurnalą. Šiame žurnale turi būti nurodyta data, taikymo sritis, kas atliko testą ir rezultatų santrauka. Jis turi būti periodiškai peržiūrimas siekiant užtikrinti nustatyto grafiko laikymąsi, pavyzdžiui, kad nė viena kritinė sistema neliktų netestuota ilgiau nei vieną metinį ciklą.

9.1 Testavimo išvadų trūkumų šalinimo pažanga turi būti stebima, o ataskaitos apie ją teikiamos kas mėnesį. Neuždarytos didelio kritiškumo problemos turi būti peržiūrimos vadovybės susitikimuose, kol bus uždarytos.

9.2 Vidaus auditas arba nepriklausomas auditorius turi kasmet peržiūrėti saugumo testavimo programą, kad patvirtintų, jog testai yra tinkamai autorizuoti, vykdomi ir apie juos tinkamai atsiskaitoma, kritinės išvados buvo pašalintos ir programa atitinka reguliavimo lūkesčius. Pavyzdžiui, auditoriai gali patikrinti, ar prieš paleidžiant naują internetinę paslaugą buvo atliktas įsiskverbimo testavimas, jei to reikalaujama. Bet kokie nukrypimai turi lemti korekcinių veiksmų planus.

10. Peržiūra ir priežiūra

10 Ši politika ir bendras testavimo planas turi būti peržiūrimi bent kartą per metus. Peržiūros metu turi būti įvertinami grėsmių aplinkos pokyčiai, pavyzdžiui, naujų atakos metodų atsiradimas, kurių dabartinis testavimas gali neapimti, ir atitinkamai koreguojama taikymo sritis arba periodiškumas.

10.1 Po bet kurio reikšmingo kibernetinio saugumo incidento ar pažeidimo ši politika turi būti peržiūrėta iš naujo, siekiant nustatyti, ar papildomas arba dažnesnis testavimas galėjo padėti išvengti problemos arba ją aptikti. Politika turi būti atnaujinta įtraukiant tokius pakeitimus, pavyzdžiui, papildant „Red Team“ pratybas nauju scenarijumi pagal stebėtus atakų dėsningumus.

10.2 Šios politikos pakeitimus turi patvirtinti vyriausiasis informacijos saugumo pareigūnas, o apie juos turi būti informuota valdyba. Apie pakeitimus turi būti informuojamas visas susijęs personalas, o išorės testavimo partneriams turi būti pranešta, jei pakeitimai daro įtaką jų pasitelkimo sąlygoms.

11. Susijusios politikos ir sąsajos

11.1 P06 – Rizikos valdymo politika. Testavimo rezultatai naudojami rizikos vertinimui ir rizikos mažinimui.

11.2 P22 – Žurnalų tvarkymo ir stebėsenos politika. Patvirtina aptikimo aprėptį pratybų metu.

11.3 P24 – Saugaus kūrimo politika. Integruoja testavimo išvadas į SDLC kontrolės priemones.

11.4 P25 – Taikomųjų programų saugumo reikalavimų politika. Užtikrina, kad reikalavimai atspindėtų testavimo metu įgytas pamokas.

11.5 P30 – Reagavimo į incidentus politika. „Red Team“ scenarijai tobulina reagavimo planus ir reagavimą.

11.6 P31 – Įrodymų rinkimo ir skaitmeninės kriminalistikos politika. Užtikrina saugų artefaktų rinkimą testavimo metu.

11.7 P32 – Veiklos tęstinumo ir atkūrimo po katastrofos politika. Pratybos patvirtina atsparumą atakos sąlygomis.

11.8 P33 – Audito ir atitikties stebėsenos politika. Užtikrina nepriklausomą testavimo programos veiksmingumo priežiūrą.

12. Nuorodos

12.1 NIS2 direktyva (ES 2022/2555), 21 straipsnio 2 dalies f punktas (politikos ir procedūros, skirtos kibernetinio saugumo rizikos valdymo priemonių veiksmingumui vertinti)

12.2 Komisijos įgyvendinimo reglamentas (ES) 2024/2690, priedo 7 skirsnis (reikalavimai kibernetinio saugumo priemonių stebėsenai, testavimui ir veiksmingumo vertinimui)

12.3 ENISA techninės gairės (2025) – priedas dėl saugumo testavimo ir audito (gairės dėl kibernetinio saugumo pratybų ir techninių testų vykdymo)

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

12.5 Pramonės geriausioji praktika: OWASP Testing Guide, NIST SP 800-115 (techninis saugumo testavimo vadovas), CBEST / GREEN Team (finansų sektoriaus „Red Team“ sistemų pavyzdžiai orientaciniam naudojimui)