					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P40					Dokumenta nosaukums: **Drošības testēšanas un red team vingrinājumu politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
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 VDAR	32. panta 1. punkta d) apakšpunkts	
ES NIS2	21. panta 2. punkta f) apakšpunkts	
ES DORA	25.–27. pants	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Mērķis

1 Noteikt strukturētu programmu organizācijas tīklu, sistēmu un lietojumprogrammu regulārai drošības testēšanai, tostarp ievainojamību izvērtēšanai, ielaušanās testēšanai un red team vingrinājumiem, lai izpildītu NIS2 direktīvas 21. panta 2. punkta f) apakšpunkta prasības attiecībā uz kiberdrošības pasākumu efektivitātes izvērtēšanu.

1.1 Nodrošināt, ka tehnisko un organizatorisko pasākumu vājās vietas tiek proaktīvi identificētas un novērstas, izmantojot kontrolētu testēšanu, tādējādi nepārtraukti uzlabojot organizācijas drošības stāvokli.

2. Piemērošanas joma

2 Šī politika attiecas uz visām organizācijai piederošām vai tās pārvaldītām kritiskajām informācijas sistēmām, lietojumprogrammām un atbalsta infrastruktūru. Tā ietver arī objektu fiziskās drošības testēšanu, ciktāl tā ir saistīta ar kiberdrošību, piemēram, sociālās inženierijas vai fiziskas iekļūšanas testus, ja tie ietilpst red team darbības jomā.

2.1 Politika ir saistoša iekšējām drošības komandām, visām nolīgtajām ārējām drošības testēšanas organizācijām un attiecīgajiem sistēmu vai lietojumprogrammu īpašniekiem. Visām testēšanas darbībām jābūt autorizētām un tās jāveic saskaņā ar šajā politikā noteiktajām procedūrām, lai nepieļautu neparedzētus darbības traucējumus.

3. Mērķi

3 Pārbaudīt ieviesto kiberdrošības kontroles pasākumu (tehnisko, darbības un organizatorisko) efektivitāti, veicot periodisku testēšanu un simulācijas atbilstoši NIS2 prasībai mērīt efektivitāti.

3.1 Atklāt ievainojamības vai trūkumus, kurus ikdienas darbības procesi var nepamanīt, tostarp nulltās dienas ievainojamības vai konfigurācijas problēmas, reālistiskos uzbrukuma scenārijos (red teaming), pirms tos izmanto apdraudējuma dalībnieki.

3.2 Sniedzot pārskatus par testu rezultātiem, nodrošināt vadībai pārliecību un īstenojamus ieteikumus, lai veicinātu informētu lēmumu pieņemšanu par riska apstrādi un drošības programmas nepārtrauktu pilnveidi.

4. Lomas un pienākumi

4 Drošības testēšanas koordinators (STC): CISO norīkota persona, kas atbild par visu drošības testēšanas darbību plānošanu un pārraudzību. Nodrošina, ka testiem ir noteikta piemērošanas joma, tie ir autorizēti un to rezultāti tiek izziņoti un izmantoti turpmākajām darbībām.

4.1 Iekšējā drošības komanda (Blue Team): piedalās testos, tostarp sniedz informāciju piemērošanas jomas noteikšanai un uzrauga sistēmas testu laikā. Red team vingrinājumos Blue Team reaģē uz simulētiem uzbrukumiem, un tiek izvērtētas tās atklāšanas un reaģēšanas spējas.

4.2 Red Team / ielaušanās testētāji: var būt iekšējā ofensīvās drošības komanda vai ārējie konsultanti. Veic testus saskaņā ar iepriekš saskaņotiem iesaistes noteikumiem, dokumentē visas atklātās ievainojamības un ekspluatācijas ceļus, kā arī nodrošina konfidencialitāti.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Uzraudzība un audits

9 STC uztur visu veikto drošības testēšanas darbību kalendāru un žurnālu. Šajā žurnālā jāiekļauj datums, piemērošanas joma, testa veicējs un rezultātu kopsavilkums. Žurnāls tiek pārskatīts, lai nodrošinātu noteiktā grafika ievērošanu, piemēram, lai neviena kritiska sistēma netiktu atstāta bez testēšanas ilgāk par gada ciklu.

9.1 Testu konstatējumu novēršanas progress tiek uzraudzīts un par to ziņots katru mēnesi. Neatrisinātās augstas smaguma pakāpes problēmas tiek pārskatītas vadības sanāksmēs līdz to slēgšanai.

9.2 Iekšējais audits vai neatkarīgs auditors katru gadu pārskata drošības testēšanas programmu, lai pārliecinātos, ka testi ir pienācīgi autorizēti, veikti un par tiem ir ziņots, kritiskie konstatējumi ir novērsti un programma atbilst regulatoru gaidām. Piemēram, auditori var pārbaudīt, vai pirms jauna tiešsaistes pakalpojuma nodošanas ražošanas vidē ir veikts ielaušanās tests, ja tas ir noteikts kā prasība. Jebkādu atkāpju gadījumā jāizstrādā korektīvo darbību plāni.

10. Pārskatīšana un uzturēšana

10 Šī politika un kopējais testēšanas plāns jāpārskata vismaz reizi gadā. Pārskatīšanā jāņem vērā izmaiņas apdraudējumu vidē, piemēram, jaunu uzbrukumu paņēmienu parādīšanās, ko pašreizējā testēšana var neaptvert, un attiecīgi jāpielāgo piemērošanas joma vai biežums.

10.1 Pēc jebkura būtiska kiberdrošības incidenta vai pārkāpuma šī politika jāpārskata atkārtoti, lai noteiktu, vai papildu vai biežāka testēšana būtu varējusi novērst vai savlaicīgi atklāt problēmu. Pēc tam politika jāatjaunina, iekļaujot nepieciešamos pielāgojumus, piemēram, pievienojot jaunu scenāriju red team vingrinājumiem, balstoties uz novērotajiem uzbrukumu modeļiem.

10.2 Šīs politikas atjauninājumi jāapstiprina CISO un jāreģistrē valdei. Visas attiecīgās personas jāinformē par izmaiņām, un ārējie testēšanas partneri jāinformē, ja kādas izmaiņas ietekmē to iesaistes nosacījumus.

11. Saistītās politikas un sasaiste

11.1 P06 – Risku pārvaldības politika. Testēšanas rezultāti veicina riska izvērtēšanu un riska apstrādi.

11.2 P22 – Žurnālfiksēšanas un uzraudzības politika. Vingrinājumu laikā validē atklāšanas pārklājumu.

11.3 P24 – Drošas izstrādes politika. Integrē testēšanas konstatējumus SDLC kontroles pasākumos.

11.4 P25 – Lietojumprogrammu drošības prasību politika. Nodrošina, ka prasības atspoguļo testēšanā gūtās atziņas.

11.5 P30 – Incidentu reaģēšanas politika. Red team scenāriji pilnveido reaģēšanas rokasgrāmatas un reaģēšanas spējas.

11.6 P31 – Digitālo pierādījumu iegūšanas un kriminālistikas politika. Nodrošina artefaktu drošu iegūšanu testēšanas laikā.

11.7 P32 – Darbības nepārtrauktības un avārijas atjaunošanas politika. Vingrinājumi pārbauda noturību uzbrukuma apstākļos.

11.8 P33 – Audita un atbilstības uzraudzības politika. Nodrošina neatkarīgu testēšanas programmas efektivitātes pārraudzību.

12. Atsauces

12.1 NIS2 direktīva (ES 2022/2555), 21. panta 2. punkta f) apakšpunkts (politikas un procedūras kiberdrošības riska pārvaldības pasākumu efektivitātes izvērtēšanai)

12.2 Komisijas Īstenošanas regula (ES) 2024/2690, pielikuma 7. sadaļa (prasības kiberdrošības pasākumu uzraudzībai, testēšanai un efektivitātes izvērtēšanai)

12.3 ENISA tehniskās vadlīnijas (2025) – pielikums par drošības testēšanu un auditu (vadlīnijas kiberdrošības vingrinājumu un tehnisko testu veikšanai)

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

12.5 Nozares labākā prakse: OWASP testēšanas rokasgrāmata, NIST SP 800-115 (tehniskā rokasgrāmata drošības testēšanai), CBEST/GREEN Team (atsaucei izmantojami finanšu nozares red teaming ietvari)