					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P40					Naslov dokumenta: **Politika varnostnega testiranja in vaj rdeče ekipe**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
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	
Uredba EU GDPR	Člen 32(1)(d)	
Direktiva EU NIS2	Člen 21(2)(f)	
Uredba EU DORA	Členi 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Namen

1 Določiti strukturiran program rednega varnostnega testiranja omrežij, sistemov in aplikacij organizacije, vključno z ocenjevanjem ranljivosti, penetracijskim testiranjem in vajami rdeče ekipe, za izpolnjevanje zahtev iz člena 21(2)(f) Direktive EU NIS2 glede ocenjevanja učinkovitosti ukrepov kibernetske varnosti.

1.1 Zagotoviti, da se pomanjkljivosti v tehničnih in organizacijskih ukrepih proaktivno prepoznajo in odpravijo z nadzorovanim testiranjem ter da se s tem stalno izboljšuje profil tveganja organizacije na področju varnosti.

2. Področje uporabe

2 Ta politika zajema vse kritične informacijske sisteme, aplikacije in podporno infrastrukturo, ki so v lasti organizacije ali jih ta upravlja. Zajema tudi testiranje fizične varnosti objektov, kadar je to relevantno za kibernetsko varnost (npr. socialni inženiring ali fizični penetracijski testi, če so vključeni v obseg vaj rdeče ekipe).

2.1 Politika velja za notranje varnostne ekipe, vse najete zunanje izvajalce varnostnega testiranja ter ustrezne lastnike sistemov in aplikacij. Vse dejavnosti testiranja morajo biti odobrene in izvedene v skladu s to politiko, da se preprečijo nenamerne motnje.

3. Cilji

3 Preverjati učinkovitost uvedenih kontrol kibernetske varnosti (tehničnih, operativnih in organizacijskih) s periodičnim testiranjem in simulacijami v skladu z zahtevo Direktive EU NIS2 glede merjenja učinkovitosti.

3.1 Odkriti ranljivosti ali vrzeli, ki jih redni operativni procesi morda ne zaznajo, vključno z ranljivostmi ničtega dne ali težavami s konfiguracijo, v realističnih scenarijih napadov (rdeče ekipe), preden jih izkoristijo akterji groženj.

3.2 Vodstvu zagotoviti zanesljivo podlago in izvedljiva priporočila s poročanjem o ugotovitvah testiranja ter s tem omogočiti informirano odločanje o obravnavi tveganj in stalno izboljševanje varnostnega programa.

4. Vloge in odgovornosti

4 Koordinator varnostnega testiranja (STC): imenuje ga vodja informacijske varnosti (CISO) in je odgovoren za načrtovanje ter nadzor vseh dejavnosti varnostnega testiranja. Zagotavlja, da so testi

ustrezno opredeljeni, odobreni, da se o rezultatih poroča in da se na njihovi podlagi izvedejo ustrezni ukrepi.

4.1 Notranja varnostna ekipa (modra ekipa): sodeluje pri testih (npr. zagotavlja informacije za določitev obsega, spremlja sisteme med testiranjem). Pri vajah rdeče ekipe se modra ekipa odziva na simulirane napade, pri čemer se ocenjujeta njena zmožnost zaznavanja in odzivanja.

4.2 Rdeča ekipa / penetracijski preizkuševalci: lahko gre za notranjo ofenzivno varnostno ekipo ali zunanje svetovalce. Teste izvajajo v skladu z dogovorjenimi pravili izvajanja, dokumentirajo vse odkrite ranljivosti in poti izkoriščanja ter varujejo zaupnost informacij.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Spremljanje in revizija

9 STC vodi koledar in dnevnik vseh izvedenih dejavnosti varnostnega testiranja. Ta dnevnik mora vključevati datum, obseg, izvajalca testiranja in povzetek rezultatov. Pregleduje se za zagotavljanje skladnosti z zahtevanim urnikom (npr. da noben kritični sistem ne ostane netestiran dlje od letnega cikla).

9.1 Napredek pri odpravi ugotovitev testiranja se spremlja in o njem poroča mesečno. Odprte ugotovitve z visoko stopnjo resnosti se obravnavajo na sestankih vodstva, dokler niso zaključene.

9.2 Notranja revizija ali neodvisni presojevalec letno pregleda program varnostnega testiranja, da preveri: ali so testiranja ustrezno odobrena, izvedena in dokumentirana; ali so bile kritične ugotovitve odpravljene; ter ali program izpolnjuje regulativna pričakovanja (na primer presojevalci lahko preverijo, ali je bilo penetracijsko testiranje izvedeno pred uvedbo nove spletne storitve, kadar je to zahtevano). Vsako odstopanje mora imeti načrt korektivnih ukrepov.

10. Pregled in vzdrževanje

10 To politiko in celotni načrt testiranja je treba pregledati najmanj enkrat letno. Pri pregledu se upoštevajo spremembe v okolju groženj (npr. pojav novih tehnik napadov, ki jih trenutno testiranje ne zajema), obseg in pogostost testiranja pa se temu ustrezno prilagodita.

10.1 Po vsakem večjem incidentu kibernetske varnosti ali kršitvi je treba to politiko ponovno pregledati, da se ugotovi, ali bi dodatno ali pogostejše testiranje lahko težavo preprečilo ali zaznalo. Politika se nato posodobi tako, da vključi takšne prilagoditve (na primer dodajanje novega scenarija v vaje rdeče ekipe na podlagi opaženih vzorcev napadov).

10.2 Posodobitve te politike mora odobriti vodja informacijske varnosti (CISO), z njimi pa mora biti seznanjen upravni odbor. O spremembah je treba obvestiti vse relevantne osebe ter zunanje partnerje za testiranje, če katera koli sprememba vpliva na pogoje njihovega sodelovanja.

11. Povezane politike in povezave

11.1 P06 – Politika upravljanja tveganj. Rezultati testiranja usmerjajo ocenjevanje in obravnavo tveganj.

11.2 P22 – Politika beleženja in spremljanja. Potrjuje pokritost zaznavanja med vajami.

11.3 P24 – Politika varnega razvoja. Ugotovitve testiranja vključuje v kontrole SDLC.

11.4 P25 – Politika zahtev za varnost aplikacij. Zagotavlja, da zahteve odražajo spoznanja iz testiranja.

11.5 P30 – Politika odzivanja na incidente. Scenariji rdeče ekipe izboljšujejo odzivne priročnike in odzivanje.

11.6 P31 – Politika zbiranja dokazov in forenzike. Omogoča varno zbiranje artefaktov med testiranjem.

11.7 P32 – Politika neprekinjenega poslovanja in obnovitve po nesreči. Vaje preverjajo odpornost med napadom.

11.8 P33 – Politika revizij in spremljanja skladnosti. Zagotavlja neodvisen nadzor nad učinkovitostjo programa testiranja.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), člen 21(2), točka (f) (politike in postopki za ocenjevanje učinkovitosti ukrepov za obvladovanje tveganj kibernetske varnosti)

12.2 Izvedbena uredba Komisije (EU) 2024/2690, Priloga, oddelek 7 (zahteve za spremljanje, testiranje in vrednotenje učinkovitosti ukrepov kibernetske varnosti)

12.3 Tehnične smernice ENISA (2025) – priloga o varnostnem testiranju in reviziji (smernice za izvajanje vaj kibernetske varnosti in tehničnih testov)

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

12.5 Najboljše prakse v panogi: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (okviri za izvajanje vaj rdeče ekipe v finančnem sektorju za referenco)