					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P40					Naziv dokumenta: **Politika sigurnosnog testiranja i vježbi crvenog tima**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
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 EU	čl. 32(1)(d)	
Direktiva EU NIS2	čl. 21(2)(f)	
Uredba EU DORA	čl. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Svrha

1 Definirati strukturirani program za redovito sigurnosno testiranje mreža, sustava i aplikacija organizacije, uključujući procjene ranjivosti, penetracijska testiranja i vježbe crvenog tima, radi ispunjavanja zahtjeva iz članka 21. stavka 2. točke (f) Direktive NIS2 koji se odnose na procjenu djelotvornosti mjera kibernetičke sigurnosti.

1.1 Osigurati da se slabosti u tehničkim i organizacijskim mjerama proaktivno utvrđuju i otklanjaju kontroliranim testiranjem, čime se kontinuirano unaprjeđuje sigurnosni profil organizacije.

2. Područje primjene

2 Ova politika obuhvaća sve kritične informacijske sustave, aplikacije i pripadajuću infrastrukturu u vlasništvu organizacije ili pod njezinim upravljanjem. Obuhvaća i testiranje fizičke sigurnosti objekata kada je to relevantno za kibernetičku sigurnost (npr. socijalni inženjering ili fizička penetracijska testiranja, ako su uključena u opseg vježbe crvenog tima).

2.1 Ova politika primjenjuje se na interne sigurnosne timove, sve ugovorene vanjske pružatelje usluga sigurnosnog testiranja te relevantne vlasnike sustava i aplikacija. Sve aktivnosti testiranja moraju biti odobrene i provoditi se u skladu s ovdje propisanim postupcima kako bi se izbjegli neželjeni prekidi.

3. Ciljevi

3 Provjeriti djelotvornost implementiranih kontrola kibernetičke sigurnosti (tehničkih, operativnih i organizacijskih) periodičnim testiranjem i simulacijama, u skladu sa zahtjevom Direktive NIS2 za mjerenje djelotvornosti.

3.1 Otkrivati ranjivosti ili nedostatke koje redoviti operativni procesi možda ne bi uočili, uključujući zero-day ranjivosti ili probleme konfiguracije, u realističnim scenarijima napada (vježbe crvenog tima) prije nego što ih akteri prijetnji iskoriste.

3.2 Pružiti rukovodstvu uvjerenje i provedive preporuke izvješćivanjem o nalazima testiranja, čime se omogućuje donošenje informiranih odluka o obradi rizika i kontinuirano unaprjeđenje programa sigurnosti.

4. Uloge i odgovornosti

4 Koordinator sigurnosnog testiranja (STC): imenuje ga glavni direktor za informacijsku sigurnost (CISO) i odgovoran je za planiranje i nadzor svih aktivnosti sigurnosnog testiranja. Osigurava da su testiranja pravilno definirana, odobrena te da se o rezultatima izvješćuje i postupa po njima.

4.1 Interni sigurnosni tim (Blue Team): sudjeluje u testiranjima (npr. pruža informacije za definiranje opsega i prati sustave tijekom testiranja). U vježbama crvenog tima Blue Team odgovara na simulirane napade, a procjenjuje se njegova sposobnost otkrivanja i odgovora.

4.2 Crveni tim / penetracijski testeri: mogu biti interni tim za ofenzivnu sigurnost ili vanjski konzultanti. Provode testiranja prema dogovorenim pravilima angažmana, dokumentiraju sve utvrđene ranjivosti i putove iskorištavanja te čuvaju povjerljivost.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Praćenje i revizija

9 STC mora voditi kalendar i evidenciju svih provedenih aktivnosti sigurnosnog testiranja. Ta evidencija treba sadržavati datum, opseg, izvršitelja testiranja i sažetak rezultata. Evidencija će se pregledavati radi potvrde poštivanja propisanog rasporeda (npr. da nijedan kritični sustav ne ostane netestiran dulje od godišnjeg ciklusa).

9.1 Napredak u otklanjanju nalaza testiranja mora se pratiti i o njemu izvješćivati mjesečno. Otvorena pitanja visoke ozbiljnosti pregledavat će se na sastancima rukovodstva sve do zatvaranja.

9.2 Unutarnja revizija ili neovisni revizor jednom godišnje pregledava program sigurnosnog testiranja kako bi provjerio jesu li testiranja pravilno odobrena, provedena i dokumentirana, jesu li kritični nalazi riješeni te ispunjava li program regulatorna očekivanja (primjerice, revizori mogu provjeriti je li penetracijsko testiranje provedeno prije pokretanja nove mrežne usluge, ako je to zahtijevano). Svako odstupanje rezultirat će planovima korektivnih radnji.

10. Pregled i održavanje

10 Ova politika i cjelokupni plan testiranja moraju se pregledati najmanje jednom godišnje. U pregledu se moraju uzeti u obzir promjene u okruženju prijetnji (npr. pojava novih tehnika napada koje trenutačno testiranje možda ne obuhvaća) te se opseg ili učestalost testiranja moraju prema potrebi prilagoditi.

10.1 Nakon svakog većeg incidenta kibernetičke sigurnosti ili povrede mora se ponovno razmotriti ova politika kako bi se utvrdilo bi li dodatno ili učestalije testiranje moglo spriječiti ili ranije otkriti predmetni događaj. Politika se potom mora ažurirati kako bi uključila takve prilagodbe (primjerice, dodavanje novog scenarija u vježbe crvenog tima na temelju uočenih obrazaca napada).

10.2 Ažuriranja ove politike mora odobriti CISO, a upravni odbor mora biti o njima obaviješten. Sve relevantno osoblje mora biti informirano o promjenama, a vanjski partneri za testiranje moraju biti obaviješteni ako promjena utječe na uvjete njihova angažmana.

11. Povezane politike i poveznice

11.1 P06 – Politika upravljanja rizicima. Rezultati testiranja služe kao podloga za vrednovanje rizika i obradu rizika.

11.2 P22 – Politika zapisivanja događaja i praćenja. Potvrđuje obuhvat otkrivanja tijekom vježbi.

11.3 P24 – Politika sigurnog razvoja. Uključuje nalaze testiranja u kontrole SDLC-a.

11.4 P25 – Politika zahtjeva sigurnosti aplikacija. Osigurava da zahtjevi odražavaju spoznaje dobivene testiranjem.

11.5 P30 – Politika odgovora na incidente. Scenariji crvenog tima unaprjeđuju operativne upute i odgovor.

11.6 P31 – Politika prikupljanja dokaza i forenzike. Omogućuje sigurno prikupljanje artefakata tijekom testiranja.

11.7 P32 – Politika neprekidnosti poslovanja i oporavka od katastrofe. Vježbe potvrđuju otpornost tijekom napada.

11.8 P33 – Politika praćenja revizije i usklađenosti. Osigurava neovisni nadzor nad djelotvornošću programa testiranja.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), članak 21. stavak 2. točka (f) (politike i postupci za procjenu djelotvornosti mjera upravljanja rizicima kibernetičke sigurnosti)

12.2 Provedbena uredba Komisije (EU) 2024/2690, Prilog, odjeljak 7. (zahtjevi za praćenje, testiranje i vrednovanje djelotvornosti mjera kibernetičke sigurnosti)

12.3 ENISA tehničke smjernice (2025.) – prilog o sigurnosnom testiranju i reviziji (smjernice za provođenje vježbi kibernetičke sigurnosti i tehničkih testiranja)

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

12.5 Najbolje prakse industrije: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (okviri za vježbe crvenog tima u financijskom sektoru, za referencu)