					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P40					Dokumentum címe: **Biztonsági tesztelési és red team szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
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	32. cikk (1) bekezdés d) pont	
NIS2 irányelv	21. cikk (2) bekezdés f) pont	
DORA rendelet	25–27. cikk	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Cél

1 Meghatározza a szervezet hálózatainak, rendszereinek és alkalmazásainak rendszeres biztonsági tesztelésére vonatkozó strukturált programot – ideértve a sérülékenységértékeléseket, a penetrációs tesztelést és a red team gyakorlatokat –, a NIS2 irányelv 21. cikk (2) bekezdés f) pontjában előírt, a kiberbiztonsági intézkedések eredményességének értékelésére vonatkozó követelmények teljesítése érdekében.

1.1 Biztosítani kell, hogy a technikai és szervezeti intézkedések gyengeségeit szabályozott teszteléssel proaktívan azonosítsák és helyesbítsék, ezáltal folyamatosan javítva a szervezet kockázati helyzetét.

2. Hatály

2 Ez a szabályzat kiterjed a szervezet tulajdonában álló vagy általa üzemeltetett valamennyi kritikus információs rendszerre, alkalmazásra és az azokhoz kapcsolódó támogató infrastruktúrára. Kiterjed továbbá a létesítmények olyan fizikai biztonsági tesztelésére is, amely kiberbiztonsági szempontból releváns (például szociális manipulációs vagy fizikai behatolási tesztek), amennyiben ezek a red team hatókörébe tartoznak.

2.1 A szabályzat az információbiztonsági csapatra, a szerződött külső biztonsági tesztelést végző szervezetekre, valamint az érintett rendszer- és alkalmazástulajdonosokra alkalmazandó. Minden tesztelési tevékenységet jóvá kell hagyni, és azt a jelen szabályzatban meghatározott eljárások szerint kell végrehajtani a nem szándékolt fennakadások elkerülése érdekében.

3. Célkitűzések

3 Az alkalmazott kiberbiztonsági kontrollok (technikai, operatív és szervezeti) eredményességét időszakos teszteléssel és szimulációkkal kell ellenőrizni, összhangban a NIS2 irányelv eredményességmérésre vonatkozó előírásaival.

3.1 Fel kell tárni azokat a sérülékenységeket vagy hiányosságokat, amelyeket a rendes működési folyamatok esetleg nem azonosítanak, ideértve a nulladik napi sérülékenységeket vagy konfigurációs problémákat is, valósághű támadási forgatókönyvek keretében (red teaming), még azt megelőzően, hogy azokat fenyegető szereplők kihasználnák.

3.2 A vezetés számára bizonyosságot és végrehajtható ajánlásokat kell biztosítani a teszteredmények jelentésével, támogatva ezzel a megalapozott kockázatkezelési döntéseket és a biztonsági program folyamatos fejlesztését.

4. Szerepkörök és felelősségek

4 Biztonsági Tesztelési Koordinátor (STC): a CISO által kijelölt szerepkör, amely felelős valamennyi biztonsági tesztelési tevékenység megtervezéséért és felügyeletéért. Biztosítja, hogy a tesztek hatóköre meghatározott és jóváhagyott legyen, továbbá hogy az eredmények dokumentálásra kerüljenek, és a szükséges intézkedések megtörténjenek.

4.1 Belső információbiztonsági csapat (Blue Team): közreműködik a tesztekben (például információt biztosít a hatókör meghatározásához, illetve felügyeli a rendszereket a tesztelés során). Red team gyakorlatok esetén a Blue Team reagál a szimulált támadásokra, és értékelés tárgyát képezi az észlelési és reagálási képessége.

4.2 Red Team / penetrációs tesztelők: lehet belső támadó biztonsági csapat vagy külső tanácsadó. A teszteket a jóváhagyott végrehajtási szabályok szerint hajtják végre, dokumentálják az összes feltárt sérülékenységet és kihasználási útvonalat, valamint megőrzik a bizalmasságot.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Nyomon követés és audit

9 Az STC naptárt és naplót vezet valamennyi végrehajtott biztonsági tesztelési tevékenységről. Ennek a naplónak tartalmaznia kell a dátumot, a hatályt, a tesztet végrehajtó személyt vagy szervezetet, valamint az eredmények összefoglalását. A naplót felül kell vizsgálni annak biztosítására, hogy az előírt ütemezés teljesüljön (például egyetlen kritikus rendszer se maradjon teszteletlenül az éves cikluson túl).

9.1 A tesztmegállapításokhoz kapcsolódó helyesbítő intézkedések előrehaladását havonta nyomon kell követni és jelenteni kell. A lezáratlan, magas súlyosságú problémákat vezetői értekezleteken kell felülvizsgálni mindaddig, amíg lezárásra nem kerülnek.

9.2 A biztonsági tesztelési programot a belső audit vagy egy független auditor évente felülvizsgálja annak ellenőrzésére, hogy a tesztek megfelelő jóváhagyással rendelkeznek, szakszerűen kerülnek végrehajtásra és jelentésre; a kritikus megállapításokat kezelték; továbbá a program megfelel a szabályozói elvárásoknak (például az auditorok ellenőrizhetik, hogy egy új online szolgáltatás indulása előtt történt-e penetrációs tesztelés, ha ez előírás). Bármely eltérés esetén helyesbítő intézkedési tervet kell készíteni.

10. Felülvizsgálat és karbantartás

10 Ezt a szabályzatot és az átfogó tesztelési tervet legalább évente egyszer felül kell vizsgálni. A felülvizsgálatnak figyelembe kell vennie a fenyegetettségi környezet változásait (például új támadási technikák megjelenését, amelyeket a jelenlegi tesztelés még nem fed le), és ennek megfelelően kell módosítani a hatályt vagy a gyakoriságot.

10.1 Bármely jelentős kiberbiztonsági incidens vagy adatvédelmi incidens után a szabályzatot ismételten felül kell vizsgálni annak meghatározására, hogy a további vagy gyakoribb tesztelés megelőzhette vagy korábban észlelhette volna-e az eseményt. A szabályzatot ezt követően frissíteni kell az ilyen módosítások beépítése érdekében (például új forgatókönyv hozzáadása a red team gyakorlatokhoz a megfigyelt támadási minták alapján).

10.2 A szabályzat módosításait a CISO hagyja jóvá, és azokról az igazgatóságot tájékoztatni kell. Minden érintett személyt értesíteni kell a változásokról, és a külső tesztelési partnereket is tájékoztatni kell, ha bármely módosítás érinti a megbízásuk feltételeit.

11. Kapcsolódó szabályzatok és összefüggések

11.1 P06 – Kockázatkezelési szabályzat. A tesztelés eredményei támogatják a kockázatértékelést és a kockázatkezelést.

11.2 P22 – Naplózási és felügyeleti szabályzat. A gyakorlatok során igazolja az észlelési lefedettséget.

11.3 P24 – Biztonságos fejlesztési szabályzat. A tesztmegállapításokat beépíti az SDLC-kontrollokba.

11.4 P25 – Alkalmazásbiztonsági követelmények szabályzata. Biztosítja, hogy a követelmények tükrözzék a tesztelés tanulságait.

11.5 P30 – Incidenskezelési szabályzat. A red team forgatókönyvek finomítják a forgatókönyveket és a reagálási képességet.

11.6 P31 – Bizonyítékgyűjtési és forenzikai szabályzat. A tesztelés során az artefaktumok biztonságos gyűjtését támogatja.

11.7 P32 – Üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabályzat. A gyakorlatok támadás alatt ellenőrzik a rezilienciát.

11.8 P33 – Audit- és megfelelésfelügyeleti szabályzat. Független felügyeletet biztosít a tesztelési program eredményessége felett.

12. Hivatkozások

12.1 NIS2 irányelv (EU 2022/2555), 21. cikk (2) bekezdés f) pont (a kiberbiztonsági kockázatkezelési intézkedések eredményességének értékelésére szolgáló szabályzatok és eljárások)

12.2 A Bizottság (EU) 2024/2690 végrehajtási rendelete, 7. mellékleti szakasz (a kiberbiztonsági intézkedések megfigyelésére, tesztelésére és eredményességének értékelésére vonatkozó követelmények)

12.3 ENISA műszaki iránymutatás (2025) – melléklet a biztonsági tesztelésről és auditról (iránymutatás kiberbiztonsági gyakorlatok és technikai tesztek végrehajtásához)

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

12.5 Iparági legjobb gyakorlatok: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (a pénzügyi szektor red teaming keretrendszerei hivatkozási célra)