PRUDENCIÁLIS MODELLEZÉSI ÉS IT FELÜGYELETI IGAZGATÓSÁG

Gyakori kérdések és válaszok sérülékenységvizsgálatok és betörési (penetrációs) tesztek végzésével kapcsolatban (GYIK)

Konzultáció

1. Van-e lehetőség a Felügyelettel konzultálni sérülékenységvizsgálatok és betörési (penetrációs) tesztek végzésével kapcsolatban?

Igen, van lehetőség a felügyeleti feladatkörében eljáró MNB-vel konzultálni. Konzultációt felügyelt intézmény az MNB kijelölt intézményi felügyelőjén keresztül, nem felügyelt intézmény (szakértő, tanácsadó stb.) pedig az Informatikai felügyeleti főosztály iff@mnb.hu e-mailcímén kezdeményezhet.

Szabályozás

2. Mi szabályozza a sérülékenységvizsgálatok és betörési (penetrációs) tesztek végzését?

A pénzügyi szektorra vonatkozó információbiztonsági követelményeket jellemzően a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló **42/2015. (III. 12.) Korm. rendelet**, illetve a vonatkozó pénzügyi ágazati törvények szabályozzák.[1]

A sérülékenységvizsgálatok és a betörési (penetrációs) tesztek végzésére vonatkozó elvárásokat az informatikai rendszer védelméről szóló (jelenleg) **8/2020. (VI.22.) MNB ajánlás** (továbbiakban: Ajánlás) 13.1.4. e) és f)[2] pontja határozza meg.

---

[1] 1 a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (a továbbiakban: Hpt.) 67. § (1) bekezdés d) pontja és 67/A. §-a,
az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 12. § (1) bekezdés d) pontja és (3) bekezdése, valamint 12/A. §-a,
a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (a továbbiakban: Bszt.) 12. §-a,
a tőkepiacról szóló 2001. évi CXX. törvény 318/D. §-a alapján a Bszt. 12. §-a,
a kollektív befektetési formákról és kezelőikről, valamint egyes pénzügyi tárgyú törvények módosításáról szóló 2014. évi XVI. törvény 29. és 30. §-a,
a magánnyugdíjról és a magánnyugdíj pénztárakról szóló 1997. évi LXXXII. törvény (a továbbiakban: Mpt.) 77/A. §-a,
az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény (a továbbiakban: Öpt.) 40/C. §-a,
a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 94. § (1) bekezdés c) pontja és (3)-(6) bekezdése,

[2] 13.1.4. e) a belső és elkülönített hálózati zónákban lévő rendszerekre vonatkozó sérülékenységvizsgálatok az intézmény belső szabályzati rendszerében meghatározott folyamat szerint legkésőbb évente, a bankkártya rendszerek, webes ügyfélkiszolgáló rendszerek, mobilalkalmazások és az azokat kiszolgáló rendszerek vonatkozásában legkésőbb negyedévente ismételve, valamint a kockázatként meghatározott kritikus hibák javítása haladéktalanul, a nem kritikus hibák javítása a kockázatokkal arányos ütemezés szerint megtörténik;

13.1.4. f) az Internet felől elérhető alkalmazások penetrációs tesztje a kockázatként meghatározott hibák javítása után, az üzembe állítást megelőzően, illetve bármely a biztonságot érintő változtatás alkalmával, majd legkésőbb évente ismételve megtörténik;

Fogalmak

3. Mit jelent a sérülékenységvizsgálat (vulnerability assessment, vulnerability scan)?

A sérülékenységvizsgálat (vulnerability assessment) célja, hogy a rendszerekben, szoftverekben vagy informatikai környezetekben azonosítsa a sérülékenységeket. Ennek egyik elterjedt, korlátozottabb formája az automatizált sérülékenységvizsgálat (vulnerability scan), melynek során automatizált eszközök használatával ellenőrzik a rendszerekben, szoftverekben az ismert biztonsági sérülékenységeket, majd jelentést készítenek az azonosított sérülékenységekről és azok kritikusságáról. A sérülékenységvizsgálat egyedüli célja a lehető legtöbb sérülékenység felderítése, azonosítása. Az azonosított sérülékenységeket a tesztelő **nem használja fel további célokra.**

4. Milyen típusai vannak a sérülékenységvizsgálatnak és melyiket kell alkalmazni?

A sérülékenységvizsgálat elvégzéséhez több fajta technika is alkalmazható. Az Ajánlás az Intézményeknek **sérülékenységvizsgálat** (vulnerability assessment) elvégzését írja elő. Az Intézmény megválaszthatja a sérülékenységvizsgálat módját, mely lehet automatizált eszközökkel végzett, vagy szakértő által lefolytatott manuális vizsgálat.

Az automatizált sérülékenységvizsgálat elvégzésének két módja van. **Autentikált**, amikor a vizsgálat a rendszerbe bejelentkezve (általában egy, a vizsgálandó rendszerben teljeskörű rendszerhozzáféréssel rendelkező felhasználóval) történik, illetve a **nem autentikált**, amikor csak a rendszer kívülről elérhető paramétereinek vizsgálata (portok, szervizek stb.) zajlik.

Az Ajánlás 13.1.4. e) pontja **nem írja elő** az automatizált sérülékenységvizsgálat módját. Az autentikált vizsgálat a rendszeren belüli elemekre is kiterjed (kiterjedése a beállított paraméterektől függ), ezért több sérülékenységet is felfedezhet, de alkalmazása előtt szükséges megvizsgálni a vizsgált rendszerre gyakorolt hatását. Az automatizált vizsgálatok a minél teljesebb körű eredmény érdekében kiegészíthetők szakértői vizsgálatokkal is.

5. Mit jelent a betörési (penetrációs) teszt?

A betörési teszt (penetrációs teszt, etikus hackelés) során egy **felhatalmazott** biztonsági szakértő különböző támadástípusokkal megvizsgálja egy rendszer, szoftver, informatikai környezet biztonságát. A tesztelő megpróbálja azonosítani és kihasználni a rendszer sérülékenységeit. A betörési teszt célja az azonosított **sérülékenységeket kihasználva** felderíteni a sérülékenységgel okozható károkat, továbbá dokumentálni a károkozáshoz vezető folyamatokat és az azok megelőzésére szükséges védelmi lépéseket.

6. Milyen típusai vannak a penetrációs tesztnek és melyiket kell alkalmazni?

A penetrációs tesztek sorában megkülönböztetünk „white-box", „grey-box", „black-box" jellegű teszteket. A „**white-box**" teszt során a tesztelő **teljes hozzáféréssel és információval**, valamint dokumentációval, illetve esetenként forráskód hozzáféréssel is rendelkezik a vizsgált rendszerre vonatkozóan. Ez a megközelítés biztosítja a legszélesebb vizsgálati lehetőséget és a rendszer legmélyebb értékelését, ugyanakkor ez szimulálja legkevésbé egy külső támadó tevékenységét. A „**Black-box**" tesztnél a tesztelőnek **semmilyen információja nincs** a vizsgált rendszerről, tevékenysége során a hozzáférési ponttól függően (internet vagy intranet) külső, vagy belső támadóként viselkedik. A „**Grey-box**" az előző két mód közötti átmenetet jelenti. A tesztelő **csak bizonyos információval** rendelkezik a rendszerről (architektúra, operációs rendszer leírás), de közvetlen adminisztrátori hozzáférése nincs.

Az Ajánlás 13.1.4. f) pontja **nem írja elő** a penetrációs teszt módját, azt az Intézménynek kell meghatároznia a kockázatokkal arányosan, figyelembe véve a fenti tesztelési módok hatásait.

7. Mit jelent a Fenyegetettség alapú behatolási teszt (Threat Led Penetration Testing - TLPT)

A TLPT egy szektor semleges behatolási teszt keretrendszer, mely nem csak a technikai rendszereket, de a folyamatokat (pl. behatolás észlelése, incidensreagálás) is teszteli. A TLTP alapján elvégzett behatolási teszteknek meg kell felelniük a keretrendszerben rögzített feltételeknek. A TLTP tesztek esetén az adott tesztelés céljának és módjának meghatározása szorosan illeszkedik ahhoz a gazdasági szektorhoz, melyben a tesztelendő Intézmény tevékenykedik (jelen esetben a pénzügyi szektorhoz), mivel a releváns fenyegetéseket szimulálja. A TLTP tesztet mindig egy független szolgáltató végzi (Red Team), időnként igénybe véve egyéb nemzeti vagy nemzetközi IT biztonsági szolgáltatók adatbázisát, esetleg közreműködését is.

8. Mit jelent a rendszerek megerősítése, biztonságnövelő konfiguráció (hardening) és hogyan történik annak ellenőrzése?

Rendszerek megerősítésének, biztonságnövelő konfigurációjának (hardening) nevezzük az egyes szállítók vagy független szakértők által a saját rendszerükhöz megadott, az alapbeállításokat felülíró, illetve kiegészítő **biztonságnövelő beállításokat** vagy ezek elvégzését. A hardening beállítások vizsgálata gyakran automatizált, történhet önállóan, de része lehet a sérülékenységvizsgálatnak is. Rendszerek megerősítésével, biztonságnövelő konfigurációjával kapcsolatban lásd még az Ajánlás 13.1.4. g) valamint specifikusan a 8.2.3. (adatbázisok) és 8.3.2. (virtuális környezetek) pontjait.

Megfelelés

9. Mely rendszerkörnyezetekben, mely rendszereken és milyen gyakorisággal szükséges sérülékenységvizsgálatokat végezni?

Az Ajánlás 13.1.4. e) pontja szerint sérülékenységvizsgálatokat a belső és elkülönített hálózati zónákban lévő rendszerekre **legkésőbb évente**, a bankkártyarendszerek, webes ügyfélkiszolgáló-rendszerek, mobilalkalmazások és az azokat kiszolgáló rendszerek vonatkozásában **legkésőbb negyedévente** szükséges elvégezni. A rendszeres sérülékenységvizsgálatokat minden rendszerre el kell végezni az **éles (produktív) rendszerkörnyezetekben**, továbbá a kockázatokkal arányos módon a nem éles (teszt, fejlesztői, oktatói) rendszerkörnyezetekben is. Az Ajánlás vonatkozó része mellett szükséges lehet figyelembe venni az egyéb, az adott rendszerre vonatkozó előírásokat (pl. PCI-DSS, SWIFT CSP) is.

A sérülékenységvizsgálatot a fejlesztések során is javasolt végezni (lásd Ajánlás 4.4.8. pontja[3]), akár többször is, kombinálva a forráskód vizsgálatával.

10. Mely rendszereken, mely rendszerkörnyezetekben milyen esetekben/gyakorisággal szükséges betörési (penetrációs) teszteket végezni?

Az Ajánlás 13.1.4. f) pontja szerint: „az Internet felől elérhető alkalmazások penetrációs tesztje a kockázatként meghatározott hibák javítása után, az **üzembe állítást megelőzően**, illetve bármely a biztonságot érintő változtatás alkalmával, majd **legkésőbb évente ismételve** megtörténik”.

„Az Internet felől elérhető alkalmazások” **körébe értendők** az Intézmény Internet felől elérhető rendszerei, alkalmazásai és az Intézmény kezelésében lévő, az Internetről elérhető eszközök (tűzfal, proxy, gateway), azzal, hogy a külső szolgáltatók saját rendszereinek (szolgáltatói útválasztók, tűzfalak, a szolgáltatók alkalmazásai) vizsgálata és a vizsgálati eredmények kiértékelése, elfogadása is része a teljeskörű sérülékenységvizsgálatnak. Ez utóbbi rendszerek vizsgálatának részleteit külön megállapodásban célszerű rögzíteni a szolgáltatókkal.

Az Internet felől nem elérhető, de kritikus adatokat feldolgozó rendszerek esetén is ajánlott a penetrációs teszt elvégzése (lásd Ajánlás 4.4.8. pontja[2]), pontja!).

Gyakorlat

11. Hogyan lehet csökkenti a penetrációs teszt hatását az éles környezetre?

Bármilyen teszt során előfordulhat nemkívánatos, előre nem látható esemény. Az éles (produktív) környezetben végzett teszteléshez **fokozott előkészület, hatástanulmány** szükséges. A penetrációs teszt elvégzését az Intézmény és a tesztelő között az Intézmény hatástanulmánya alapján létrejövő megállapodáshoz vagy engedélyhez kell kötni, aminek legalább az alábbiakat kell tartalmaznia:

[3] 4.4.8. Az intézmény gondoskodik a megváltoztatott informatikai rendszerek, rendszerelemek, paraméterek éles üzembe állítását megelőző, dokumentált, elvárható gondosságú teszteléséről. A tesztelés során az intézmény gondoskodik a funkcionális és a nem funkcionális tesztek elvégzéséről, beleértve az informatikai biztonsági teszteket is.

- milyen rendszerek vizsgálata történik;
- milyen típusú penetrációs teszt készül;
- mennyi ideig tart a teszt;
- ki végzi el a tesztelést;
- milyen eszközökkel történik a tesztelés;
- milyen mélységű a tesztelés (milyen információ és bizonyosság megszerzése után kell abbahagyni a tesztelést).

A fenti paraméterek megadásával az Intézmény az éles üzemi rendszere működéséhez tudja igazítani a penetrációs teszt elvégzését. Emellett célszerű a tesztelés ideje alatt elérhető vészhelyzeti kapcsolattartók személyében és elérhetőségében is megállapodni, hogyha nemkívánatos esemény következik be, annak hatását minimalizálni lehessen.

12. Szükséges-e a tesztelőknek számlát, fiókot nyitnia, ügyféllé válnia (például éles internetbank, mobilbank, partnerportál vagy ügyfélportál tesztelése esetén)?

A penetrációs teszt egyik célja annak feltérképezése, hogy az ügyfél csak a neki megengedett üzleti logika mentén tudja a rendszert használni, vagy attól eltérő, a jogosultsági szintjét meghaladó mértékben is. A tesztelőnek a vizsgálat elvégzéséhez szükséges hozzáférnie **a felhasználók által használt felülethez**, hogy az ott elvégezhető műveletek paramétereinek módosításával felderíthesse az esetleges programhibákat, hibás konfigurációt és a visszaélési lehetőségeket (limit kikerülés, más nevében való tranzakció stb.). Ennek biztosítására szükséges lehet a tesztelőknek számlát, fiókot nyitnia, ügyféllé válnia, vagy a tesztelő részére egy külön bejelentkezési lehetőséget kell biztosítani. Bizonyos esetekben a leghatékonyabb mód az éles rendszeren való tesztelés, ugyanakkor az üzleti feltételek teljesítése akadályozhatja a technikai vizsgálatok teljeskörűségét. Az Intézmény hatáskörébe tartozik annak az eldöntése a kockázatokat mérlegelve, hogy a tesztelő számlát, fiókot nyit, ügyféllé válik (és a tesztelést jól behatárolt, előre egyeztetett, előkészített módon, különös körültekintés mellett végzi-e), vagy tevékenységét tudja-e elkülönítve kezelni az éles rendszerben, és a tesztelési adatok tárolása, feldolgozása, törlése kihatással lehet-e a jogszabályi és egyéb megfelelésre. Amennyiben a tesztelő tevékenysége ilyen szempontból a kockázatokkal arányosan teljeskörűen nem valósítható meg, nem szabályozható, illetve a tesztadatok kezelése nem oldható meg az éles rendszerben, úgy az Intézmény a 13. pontban foglaltak alapján köteles eljárni.

13. Mi történik, ha az Intézmény véleménye szerint a penetrációs teszt elvégzése túl kockázatos az éles rendszeren?

Az éles rendszeren való tesztelés biztosítja a leghatékonyabban a tesztelőnek azt a lehetőséget, hogy a teszt során egy támadó szemszögéből vizsgálja a rendszer biztonságát. Minden egyéb, az éles rendszeren kívüli teszt egy vagy több, az éles rendszerben található hiba figyelmen kívül hagyását eredményezheti. Emellett a rendszerkapcsolatok, adatkapcsolatok és folyamatok (pl. TLPT esetén) gyakran csak az éles rendszereken tesztelhetők, ezért egyes módszertanok (pl. TIBER-EU) elő is írják, hogy a teszteket az éles rendszereken kell végezni.

Amennyiben az Intézmény a penetrációs tesztek egy részének vagy egészének futtatását a tesztelési módok mindegyikével megfelelően megalapozott indokok alapján az éles rendszeren túl kockázatosnak ítéli, akkor elvégezheti azt **az éles rendszerrel teljesen azonos környezetben** is. Ilyen esetben az Intézménynek dokumentáltan bizonyítani kell, hogy a teszthez használt környezet a teszt szempontjából megegyezik az éles környezettel.

Jó gyakorlatnak számít egy rendszert közvetlenül az élesítés előtt tesztelni, mikor már nem várhatók benne további módosítások.

Amennyiben a mélyebb betörési teszteket nem az éles rendszerkörnyezetben végzi az Intézmény, akkor szükséges lehet az éles és a vizsgált rendszerkörnyezetben a rendszer és futtatókörnyezet konfigurációjának white-box jellegű összevetése, továbbá a betörési teszt során feltárt hiányosságok javításának visszaellenőrzése (retest) a kockázatokkal arányos mértékben az éles rendszerkörnyezetben is.

14. Hogyan lehet arról meggyőződni, hogy a tesztrendszer nem tér el a sebezhetőségi vizsgálat szempontjából az éles rendszertől?

Amennyiben az Intézmény a penetrációs tesztek egy részének vagy egészének futtatását a tesztelési módok mindegyikével megfelelően megalapozott indokok alapján az éles rendszeren túl kockázatosnak ítéli, akkor az éles rendszerkörnyezettel való azonosságról, illetve a tesztelés hatékonyságát és eredményességet érdemben nem befolyásoló vagy gátló eltérésekről az alábbiak ellenőrzése révén kell dokumentáltan bizonyosságot szerezni:

- verziókezelés/-követés;
- alkalmazáskonfiguráció, technikai paraméterek az éles és a vizsgált környezetben;

- telepítési (implementációs) és tesztelési dokumentáció;
- üzemeltetési dokumentáció;
- rendszerkörnyezeteket, architektúrát és az interfészeket (integráció szintjét) bemutató dokumentumok;
- éles és vizsgált környezet szempontjából releváns beállítások és szabályok a határvédelmi, hálózatbiztonsági rendszerekből;
- felhasználói és jogosultsági lista az éles és a vizsgált környezetben;
- mappajogosultságok (amennyiben az alkalmazás szempontjából releváns) az éles és a vizsgált környezetben;
- hardening és sérülékenységvizsgálati jegyzőkönyv az éles és a vizsgált környezetre.

A bizonyossághoz alátámasztó dokumentumok, evidenciák bekérése és vizsgálata is szükséges (például konfigurációs állományok, tanúsítványok, képernyőképek).

15. Pénzmosás megelőzési szempontból milyen szabályokat kell figyelembe venni, ha éles rendszerben történik a biztonsági tesztelés?

A pénzmosás és terrorizmus-finanszírozás elleni elvárásokat a 2017. évi LIII. törvény, valamint az azt kiegészítő rendeletek (21/2017. NGM Rendelet, 26/2020. MNB Rendelet) és további felügyeleti ajánlások határozzák meg. Ezen felül az MNB az egységes jogértelmezés elősegítése érdekében Q&A felületet is kialakított, továbbá egyéb segédleteket adott ki.