SÉRÜLÉKENYSÉGVIZSGÁLATI METODIKÁK

Belső hálózat és rendszerek vizsgálata

v 1.0

Hatályos:

Digitálisan aláírta: Kiss Tamás László
Dátum: 2026.10.12 07:32:37 +02'00'

Kiss Tamás László
Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Sérülékenységvizsgálati Főosztály

Figyelem! A dokumentum érzékeny információkat tartalmazhat!

1. Vizsgálatok összefoglaló leírása

A **belső hálózati** irányultság keretében a rendszerek ellenőrzése egyedi módszertan szerint történik. A vizsgálatok alapját automatizált sérülékenység-felderítő eszközök eredményei képezik, amelyeket a vizsgált rendszer technológiai sajátosságainak megfelelő, célzott manuális biztonsági tesztelés egészít ki.

A vizsgálat az alábbi fő tesztelési területekre terjed ki:

- Információgyűjtés és hálózatfelderítés;
- Hálózati infrastruktúra vizsgálata;
- Rendszerek és szolgáltatások azonosítása;
- Konfiguráció- és üzemeltetésbiztonság vizsgálata;
- Hitelesítési mechanizmusok vizsgálata;
- Hozzáférés-védelmi mechanizmusok vizsgálata;
- Hálózati kommunikáció elemzése.

Az informatikai rendszerek belső sérülékenységvizsgálata belső hálózati végpontról (vagy közvetve távoli hozzáféréssel) az alábbiak szerint, két fázisban kerül végrehajtásra.

Első fázis (regisztrált felhasználói jogosultság nélküli felderítés):

- Információgyűjtés;
- Hálózati címzési struktúra feltérképezése;
- Hálózati hozzáférés-védelmi mechanizmusok feltérképezése;
- A hálózatban elérhető rendszerek feltérképezése;
- Az elérhető eszközök operációs rendszereinek, szolgáltatásainak, illetve verzióinformációinak azonosítása;
- Nyilvános sérülékenységi adatbázisok alapján listák készítése a vizsgált szolgáltatásokat érintő biztonsági hibákról;
- Hálózati forgalom lehallgatása és elemzése, amennyiben szükséges közbeékelődéses (man-in-the-middle) technikák alkalmazásával;
- Hálózati szegmentációs, valamint határvédelmi megoldások vizsgálata, beleértve azok szabályrendszerének megkerülhetőségi ellenőrzését;
- Hitelesítési adatok, azonosítók, illetve jelszavak felderítése és azok erősségének, valamint kihasználhatóságának vizsgálata;
- A fentiekben szerzett információk elemzése és további manuális vizsgálat elvégzése.

Második fázis (jogosultsággal végzett vizsgálatok):

- Dokumentáció és konfigurációk validálása;
- Rendszerek és szolgáltatások feltérképezése;
- Operációs rendszerek és alkalmazások biztonsági vizsgálata;
- Javításkezelési folyamatok és frissítések vizsgálata;

- Hitelesítési követelmények és jelszóházirendek vizsgálata;
- Jelszavak visszafejthetőségének vizsgálata.

Az **eszköz- és szoftverkonfigurációs ellenőrzések** során az érintett rendszerek beállításainak felülvizsgálata történik a biztonsági követelményeknek való megfelelés érdekében. A vizsgálatok alapját a Central for Internet Security (CIS) ajánlásai, valamint a vonatkozó gyártói útmutatók képezik. Az ellenőrzés kiterjed a biztonsági beállításokra, a hozzáférés-kezelésre, a menedzsmentfunkciókra, a naplózásra és a rendszerek naprakészségére.

2. Vizsgálatok részletes műszaki leírása

2.1 Hálózat felderítése - (LOC-NET-INFO-001)

Annak vizsgálata, hogy a hálózatban milyen kapcsolatok észlelhetők.

2.2 Végpontok felderítése - (LOC-NET-INFO-002)

Annak vizsgálata, hogy a hálózatban milyen végpontokat lehet beazonosítani.

2.3 Szolgáltatások felderítése - (LOC-NET-INFO-003)

Annak vizsgálata, hogy a hálózatban milyen szolgáltatások érhetők el.

2.4 Szoftverkörnyezet felderítése - (LOC-NET-INFO-004)

Annak vizsgálata, hogy a hálózat végpontjaira telepített operációs rendszerek és alkalmazások naprakészek-e.

2.5 Hálózati hozzáférés vizsgálata - (LOC-NET-INFO-005)

Annak vizsgálata, hogy a hálózat végpontjai megfelelően védettek-e a hálózatról történő kompromittálás ellen.

2.6 Hálózati forgalom tartalmának vizsgálata - (LOC-NET-INFO-006)

Annak vizsgálata, hogy a hálózat végpontjainak forgalmából lehallgathatók-e potenciálisan érzékeny adatok.

2.7 Rendszerrel kapcsolatos dokumentáció felderítése - (LOC-NET-INFO-007)

Annak vizsgálata, hogy a hálózat végpontjainak dokumentációi vagy topológiája elérhető-e és ezekből milyen adatok ismerhetők meg.

2.8 Hálózati végpont konfigurációjának vizsgálata - (LOC-NET-CONF-001)

Annak vizsgálata, hogy a hálózat végpontjai megfelelően kerültek-e beállításra.

2.9 Infrastruktúra és alkalmazás adminisztrátori interfészek vizsgálata - (LOC-NET-CONF-002)

Annak vizsgálata, hogy a hálózat végpontjainak működése szempontjából kritikus felületek szabadon hozzáférhetők-e.

2.10 Naplózás vizsgálata - (LOC-NET-CONF-003)

Annak vizsgálata, hogy a hálózat végpontjain végzett műveletek megfelelően kerülnek-e naplózásra.

2.11 Szegmentáció vizsgálata - (LOC-NET-CONF-004)

Annak vizsgálata, hogy a hálózat végpontjait összekötő alhálózatok megfelelően elkülönítettek-e.

2.12 Szegregáció vizsgálata - (LOC-NET-CONF-005)

Annak vizsgálata, hogy a hálózat végpontjainak egymással való kommunikációja megfelelően került-e beállításra.

2.13 Hálózati végpont védelmének vizsgálata - (LOC-NET-CONF-006)

Annak vizsgálata, hogy a hálózat végpontjainak védelmi rendszere megfelelően került-e beállításra.

2.14 Hálózati jogosultságkezelés vizsgálata - (LOC-NET-CONF-007)

Annak vizsgálata, hogy a hálózatra történő csatlakozás esetén a felhasználók mely feltételek teljesülése esetén hajthatnak végre műveleteket.

2.15 Felhasználói hozzáférés és jogosultságok vizsgálata - (LOC-NET-CONF-008)

Annak vizsgálata, hogy a hálózatban megfelelően kerültek-e kialakításra a felhasználói hozzáférések és jogosultságok.

2.16 Jelszószabályok vizsgálata - (LOC-NET-CONF-009)

Annak vizsgálata, hogy a hálózatban megfelelően kerültek-e kialakításra a jelszó házirendek.

2.17 Szoftverfrissítések ellenőrzése - (LOC-NET-CONF-010)

Annak vizsgálata, hogy a hálózat végpontjainak operációs rendszerei és alkalmazásai tekintetében rendszeres vagy időszakos frissítési folyamatok kerültek-e beállításra.

2.18 Adatbázis biztonságának vizsgálata - (LOC-NET-CONF-011)

Annak vizsgálata, hogy a hálózat végpontjainak adatbázisai megfelelően védettek-e.

2.19 Behatolásérzékelő rendszerek biztonsági vizsgálata - (LOC-NET-CONF-012)

Annak vizsgálata, hogy a hálózatot monitorozó behatolásérzékelő rendszer megfelelően került-e beállításra.

2.20 Terhelésérzékelő rendszerek biztonsági vizsgálata - (LOC-NET-CONF-013)

Annak vizsgálata, hogy a hálózatot monitorozó terhelésérzékelő rendszer megfelelően került-e beállításra.

2.21 Távoli elérési módok biztonsági vizsgálata - (LOC-NET-CONF-014)

Annak vizsgálata, hogy a hálózat távoli eléréséhez használt kapcsolat megfelelően került-e beállításra.

2.22 Védelmi szolgáltatások vizsgálata - (LOC-NET-CONF-015)

Annak vizsgálata, hogy a hálózat védelmi rendszere megfelelően került-e beállításra.

2.23 Dokumentáció és rendszerleírás felderítése - (LOC-DEV-INFO-001)

Annak vizsgálata, hogy a munkaállomás dokumentációja vagy valamely rendszerének leírása feltárható-e.

2.24 Fizikai biztonság és hozzáférés elleni védelem felderítése - (LOC-DEV-INFO-002)

Annak vizsgálata, hogy a munkaállomás megfelelő fizikai biztonsággal és hozzáférés elleni védelmmel rendelkezik-e.

2.25 Rendszerbetöltési folyamat felderítése - (LOC-DEV-INFO-003)

Annak vizsgálata, hogy a munkaállomás operációs rendszerét betöltő alrendszer megfelelően védett-e.

2.26 Szolgáltatások felderítése - (LOC-DEV-INFO-004)

Annak vizsgálata, hogy a munkaállomás szolgáltatásai megfelelően védettek-e.

2.27 Szoftverkörnyezet felderítése - (LOC-DEV-INFO-005)

Annak vizsgálata, hogy a munkaállomás operációs rendszere és alkalmazásai naprakészek-e.

2.28 Tárolt adatok felderítése - (LOC-DEV-INFO-006)

Annak vizsgálata, hogy a munkaállomás tárterületéről potenciálisan érzékeny adatok felderíthetők-e.

2.29 Rendszer konfiguráció vizsgálata - (LOC-DEV-CONF-001)

Annak vizsgálata, hogy a munkaállomás szolgáltatásai és alkalmazásai megfelelően kerültek-e beállításra.

2.30 Hálózat vizsgálata - (LOC-DEV-CONF-002)

Annak vizsgálata, hogy a munkaállomás adataiból feltárhatók-e információk az eszköz eredeti hálózati struktúrájáról, illetve korábbi hálózati kommunikációjáról.

2.31 Védelmi szoftverek vizsgálata - (LOC-DEV-CONF-003)

Annak vizsgálata, hogy a munkaállomás végpontvédelmi rendszere megfelelően került-e beállításra.

2.32 Biztonsági adatmentés vizsgálata - (LOC-DEV-CONF-004)

Annak vizsgálata, hogy a munkaállomás felületén biztonsági adatmentő folyamat került-e kialakításra.

2.33 Rendszer és alkalmazás frissítési folyamatok vizsgálata - (LOC-DEV-CONF-005)

Annak vizsgálata, hogy a munkaállomás operációs rendszere és alkalmazásai tekintetében rendszeres vagy időszakos frissítési folyamatok kerültek-e beállításra.

2.34 Naplózás vizsgálata - (LOC-DEV-CONF-006)

Annak vizsgálata, hogy a munkaállomás felületén végzett műveletek megfelelően kerülnek-e naplózásra.

2.35 Távoli elérések konfigurációjának vizsgálata - (LOC-DEV-CONF-007)

Annak vizsgálata, hogy a munkaállomás távoli elérésének konfigurációja megfelelően került-e beállításra.

2.36 Adatbázis biztonságának vizsgálata - (LOC-DEV-CONF-008)

Annak vizsgálata, hogy a munkaállomás adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.37 Bejelentkezési folyamat vizsgálata - (LOC-DEV-AUTN-001)

Annak vizsgálata, hogy a munkaállomás bejelentkezési folyamata megkerülhető-e, ahhoz jelszóemlékeztető megismerhető-e.

2.38 Alapértelmezett hitelesítési adatok vizsgálata - (LOC-DEV-AUTN-002)

Annak vizsgálata, hogy a munkaállomás alkalmazásaiban az alapértelmezetten használt felhasználók elérhetők-e.

2.39 Felhasználói fiókok vizsgálata - (LOC-DEV-AUTN-003)

Annak vizsgálata, hogy a munkaállomáson megfelelően kerültek-e kialakításra a felhasználói hozzáférések és jogosultságok.

2.40 Kizárási házirend vizsgálata - (LOC-DEV-AUTN-004)

Annak vizsgálata, hogy a munkaállomás szankcionálja-e a helytelen bejelentkezési kísérleteket.

2.41 Jelszószabályok vizsgálata - (LOC-DEV-AUTN-005)

Annak vizsgálata, hogy a munkaállomás jelszó házirendjei megfelelően kerültek-e kialakításra.

2.42 Jogosultságkezelés megkerülésének vizsgálata - (LOC-DEV-AUTZ-001)

Annak vizsgálata, hogy a munkaállomás bizonyos jogosultsági szint birtokában elérhető funkciói hozzáférhetők-e az elvártnak nem megfelelő jogosultsági szint birtokában.

2.43 Jogosultság kiterjesztés vizsgálata - (LOC-DEV-AUTZ-002)

Annak vizsgálata, hogy a munkaállomás felhasználói hozzájuthatnak-e a számukra kiosztottnál bővebb jogosultságokhoz.

2.44 Felhasználói hozzáférések szabályainak vizsgálata - (LOC-DEV-AUTZ-003)

Annak vizsgálata, hogy a munkaállomáshoz csatlakoztatható-e írási és végrehajtási jogosultsággal külső eszköz.

2.45 Kommunikációs protokollok vizsgálata - (LOC-DEV-NETW-001)

Annak vizsgálata, hogy a rendszer hálózati protokolljai és kommunikációs szolgáltatásai megfelelnek-e a biztonsági követelményeknek, valamint alkalmaznak-e elavult vagy nem biztonságos megoldásokat.

2.46 Hitelesítési és érzékeny adattovábbítás vizsgálata - (LOC-DEV-NETW-002)

Annak vizsgálata, hogy a rendszer a hitelesítési adatokat és az egyéb érzékeny információkat a hálózati kommunikáció során megfelelően védi-e, valamint azok megszerezhetők-e vagy módosíthatók-e jogosulatlanul.

2.47 Gyenge titkosítás vizsgálata - (LOC-DEV-NETW-003)

Annak vizsgálata, hogy a rendszer megfelelően biztonságos kriptográfiai algoritmusokat használ-e.