

Kiberbiztonsági gyakorlatok általános módszertana

A jelen módszertan a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Kiberbiztonsági vhr.) 10. §-ának előírásai alapján készült, és hatálya a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdése szerinti szervezetekre terjed ki. Ezen szervezetek számára nyújt útmutatót a kötelezően, hatósági vagy központi kötelezés alapján lefolytatandó, valamint az önállóan szervezett kiberbiztonsági gyakorlatok tervezéséhez, lebonyolításához és értékeléséhez. A gyakorlatok célja, hogy növeljék a szervezetek kiberfenyegetések megelőzésével, felismerésével és kezelésével kapcsolatos felkészültségét, valamint teszteljék a döntéshozatali és kommunikációs folyamatokat valósághű környezetben. Ezzel biztosítható a jogszabályi megfelelés és a folyamatos szervezeti fejlődés.

Ezen módszertan irányadó az alábbi szervezetekre:

- A Kiberbiztonsági tv. 1. mellékletében felsorolt közigazgatási ágazathoz tartozó szervezetek,
- A többségi állami befolyás alatt álló gazdálkodó szervezetek, a Kiberbiztonsági tv. 1. § (1) bekezdés ba) és bb) pontjaiban meghatározott küszöbértékek esetén,
- A nemzeti vagy honvédelmi kiberbiztonsági hatóság által azonosított alapvető vagy fontos szervezetek,
- A Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezetek, ha középvállalkozásnak minősülnek, vagy ha a Kiberbiztonsági tv. 1. § (1) bekezdés da) vagy db) pontjaiban meghatározott küszöbértékeknek megfelelnek,
- Elektronikus hírközlési szolgáltató, bizalmi szolgáltató, DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó, doménnév-regisztrációt végző szolgáltató,
- Honvédelmi érdekekhez kapcsolódó tevékenységet folytató gazdasági társaság.

Kivétel:

- A minősített adatot kezelő vagy műveleti célú rendszerek, illetve azon külön jogszabályban meghatározott speciális kiberbiztonsági szolgáltatások, amelyekre más előírások vonatkoznak.

Kiberbiztonsági gyakorlat lefolytatásának esetei:

- Kötelezően kétfévente: a Kiberbiztonsági tv. 1. § (1) bekezdése szerinti alapvető szervezetnek,
- Nemzeti kiberbiztonsági incidenskezelő központ (a továbbiakban: Központ) kötelezése alapján,
- Nemzeti Kiberbiztonsági Intézet (a továbbiakban: NKI) kötelezése alapján.

A szervezet vezetőjének feladata, hogy biztosítsa a kötelezően előírt kiberbiztonsági gyakorlatokon történő részvételt, illetve kiberbiztonsági gyakorlat önálló megtartását.

A módszertan nyilvánosan közzétehető keretrendszer biztosít, amelyet a szervezetek saját kockázati környezetükhöz és erőforrásaikhoz igazíthatnak. A dokumentum tartalma az alkalmazási tapasztalatok, a kiberfenyegetettségi környezet változásai, valamint a vonatkozó jogszabályi és szakmai követelmények módosulása esetén felülvizsgálatra kerülhet. A

módszertant kidolgozó és közzétevő szerv fenntartja a módosítás jogát, ideértve különösen a módszertani elemek pontosítását, kiegészítését, aktualizálását és szerkesztési jellegű módosítását. A mindenkor hatályos, közzétett változat alkalmazása irányadó a gyakorlatok tervezése, lebonyolítása, értékelése és utókövetése során.

Szerepkörök és elhatárolás

Különösen fontos, hogy a gyakorlat két, egymástól szigorúan elkülönített szerepkörre épüljön. Az első szerepkörbe tartoznak a szervezők, akik felelősek a tervezésért, a lebonyolítás irányításáért és az értékelési folyamat elvégzéséért. A második szerepkörbe tartoznak a játékosok, akik a gyakorlatot végrehajtják, a scenárióra reagálnak, és a szervezet tényleges működési folyamatai szerint hajtják végre a döntéseket. A két szerepkör nem keveredhet, és egyik résztvevő sem láthat el egyszerre szervezői és játékos feladatot. Ez az elhatárolás biztosítja, hogy a gyakorlat során ne keletkezzen összeférhetetlenség, ne sérüljön az objektivitás, és a későbbi értékelés hiteles és visszakövethető legyen. A szerepkörök szétválasztását minden esetben írásban kell rögzíteni a gyakorlat tervezési fázisában, hogy a felelősségi határok minden érintett számára egyértelműek legyenek.

Szervezők

A szervezők végzik a gyakorlat szakmai előkészítését, a lebonyolítás irányítását és az értékelést. A szervezők feladatai:

- a célok meghatározása,
- a scenárió és részletes forgatókönyv kidolgozása,
- a gyakorlat teljes technikai és szervezési felügyelete,
- a megfigyelés és dokumentálás,
- az értékelés és a fejlesztési javaslatok elkészítése.

A szervezői funkciót elláthatja:

- **külső, független szakmai szervezet** (ideális megoldás),
- vagy **belső, elkülönített csapat**, amely **semmilyen formában nem vehet részt játékosként**, és nem lehet része az incidenskezelési, kommunikációs vagy vezetői folyamatoknak.

A szervezők és játékosok között **tilos a szerepkörök átfedése**. A szervező nem lehet játékos, a játékos nem férhet hozzá a forgatókönyvhöz, nem vehet részt a tervezésben és értékelésben sem.

Az elhatárolást minden gyakorlat előtt **írásban kell rögzíteni**, név szerint kijelölve:

- ki a tervező,
- ki a lebonyolító,
- ki az értékelő,
- kik a játékosok,
- hogyan biztosított a függetlenség és az összeférhetetlenség kizárása.

Játékosok

A játékosok az adott szervezet tényleges reagáló szereplői, akik a gyakorlat során:

- incidenseket kezelnek,
- döntéseket hoznak,
- kommunikálnak,
- együttműködnek.

A játékos csoport kötelező minimum összetétele:

- **egy játékos vezető** (döntéshozó, általában vezető beosztású személy),
- **legalább két incidenskezelő** (technikai és operatív reagálók),
- **sajtókommunikációért felelős személy**,
- **jogi szakember**, aki tisztában van a hatályos kiberbiztonsági és adatvédelmi jogszabályokkal.

A játékosok **valós feladataik szerint** működnek, és nincsenek tudatában a teljes forgatókönyvnek, csak az általuk észlelt eseményekkel találkoznak.

A gyakorlat tervezése

A kiberbiztonsági gyakorlat előre megtervezett és szervezett tevékenység, amely a szervezet kiberbiztonsági felkészültségének, reagálási képességeinek és kommunikációs mechanizmusainak valóságú környezetben történő tesztelésére irányul. A tervezést minden esetben a szervezők végzik, a játékosok bevonása nélkül. A tervezés célja, hogy a gyakorlat világos keretek között, meghatározott célok mentén, mérhető eredményekkel járjon, és a szervezet működéséhez illeszkedjen.

A tervezési folyamat első lépése a gyakorlat céljainak meghatározása. A szervezetnek egyértelműen ki kell jelölnie, hogy a gyakorlat milyen képességeket kíván tesztelni, például az incidenskezelés hatékonyságát, a belső és külső kommunikáció működését, a technikai védekezési mechanizmusok reagálási képességeit vagy a vezetői döntéshozatal pontosságát. A világosan megfogalmazott célkitűzések biztosítják, hogy az eredmények objektíven mérhetők és értékelhetők legyenek.

A következő lépés a forgatókönyv (szcenárió) kialakítása. A forgatókönyv valóságú kiberfenyegetést vagy incidenst modellez, amely során vizsgálható a szervezet működési folyamata. A scenáriónak tartalmaznia kell a kiinduló helyzetet, az események logikai láncolatát és az elvárt reakciókat. A tervezés során figyelembe kell venni a szervezet valós működési környezetét és kockázati tényezőit, ugyanakkor a gyakorlat nem okozhatja a működés ellehetetlenülését. A valóságosság és az arányosság elvének együtt kell érvényesülnie.

A dokumentációban kötelező rögzíteni, hogy ki mely szerepben vesz részt a gyakorlatban, és azt is, hogy a szerepekhez tartozó feladatok nem fedhetik egymást. A szerepkörök közötti szigorú elválasztás biztosítja a gyakorlat hitelességét, valamint a későbbi értékelés objektívitasát és visszakövethetőségét.

Amennyiben a gyakorlat lebonyolításába külső szakértő (például tréningcég, szaktanácsadó vagy az NKI) is bevonásra kerül, az együttműködés feltételeit és a felelősségi határokat írásos megállapodásban kell rögzíteni. A megállapodásnak tartalmaznia kell a szervezők és a külső közreműködők pontos szerepeit, a feladatok és hatáskörök elhatárolását, az adatkezelés és információbiztonság követelményeit, valamint a bizalmasságra és összeférhetlenségre vonatkozó szabályokat.

A tervezés része a gyakorlat időkeretének, ütemezésének és erőforrásigényének meghatározása is. A tervezési dokumentumoknak biztosítaniuk kell, hogy a gyakorlat ne okozzon aránytalan fennakadást a szervezet mindennapi működésében, ugyanakkor elegendő időt és teret adjon a felkészültség valós vizsgálatára.

A tervezés teljes folyamatáról, beleértve a döntéseket, egyeztetéseket, jóváhagyásokat és a véglegesített forgatókönyvet, írásos nyilvántartást kell vezetni. Ez a nyilvántartás a lebonyolítás, az értékelés és az utólagos ellenőrzések során alapvető hivatkozási dokumentum.

A tervezési szakasz teremti meg azt a szervezeti, logikai és dokumentációs keretet, amely biztosítja, hogy a gyakorlat lebonyolítása ne improvizatív módon, hanem tudatosan, mérhetően és ellenőrizhetően történjen.

A gyakorlat lefolytatása

A kiberbiztonsági gyakorlat lebonyolítása a tervezési szakaszban rögzített forgatókönyv alapján, szervezett és dokumentált keretek között zajlik. A cél a szervezet reagálási, döntéshozatali és kommunikációs képességeinek valós körülményekhez közeli vizsgálata, olyan módon, hogy a kialakított szabályok, szerepkörök és elhatárolások minden pillanatban érvényesüljenek.

A lebonyolítás első szakasza a megnyitás és az előkészítés. Ekkor a szervezők ismertetik a gyakorlat céljait, szabályait, időkeretét és a résztvevők feladatait, minden esetben írásban is rögzítve ezeket. A gyakorlat megkezdése előtt minden szereplőnek írásban kell nyilatkoznia arról, hogy megismerte a számára meghatározott hatásköröket, a korlátokat és az összeférhetetlenségi szabályokat. Ez biztosítja, hogy a folyamat átlátható és visszakövethető legyen, valamint, hogy a lebonyolítás során ne merülhessen fel olyan beavatkozás, amely a gyakorlat hitelességét veszélyeztetné.

A második szakasz a szcenárió végrehajtása, amely a gyakorlat központi eleme. A szervezők a forgatókönyv alapján indítják és vezetik be az egyes eseményeket, miközben folyamatosan figyelik a játékosok reakcióit. A játékosok a valós munkarendjük szerint kezelik az eseményeket, döntenek és kommunikálnak.

A kommunikáció és a koordináció vizsgálata is itt történik meg. A szervezők értékelik, hogy az információk milyen gyorsan és pontosan jutnak el a szervezet különböző szintjeihez, hogy a külső partnerekkel, szolgáltatókkal és hatóságokkal való együttműködés mennyire hatékony, és hogy a belső kommunikáció megfelel-e a szervezet szabályainak és jogi kötelezettségeinek.

A szervezők feladata a folyamatos és részletes dokumentálás. A folyamat minden elemét írásban kell rögzíteni, beleértve a félreértéseket, az elakadásokat és az esetleges kommunikációs hibákat is, mivel ezek fontos visszajelzést adnak a szervezeti működés érettségéről és fejlesztési szükségleteiről. Rögzíteni kell a játékosok által tett lépéseket, azok időpontját, a döntések indokait és a felmerült nehézségeket. A dokumentáció célja, hogy a gyakorlat értékelése objektív alapokra épülhessen, ezért minden eseményt pontosan és ellenőrizhető módon kell lejegyezni. A gyakorlat lezárását követően a dokumentáció releváns részeit ismertetni szükséges a játékosokkal, különös tekintettel a döntési pontokra, az elakadásokra és a kommunikációs tapasztalatokra. Ez lehetőséget biztosít a közös tanulságok levonására, az egyéni és szervezeti fejlődési irányok azonosítására, valamint a jövőbeni működés tudatos és mérhető fejlesztésére.

A lebonyolítás záró szakaszában a szervezők hivatalosan lezárják a gyakorlatot. A gyakorlatvezető ekkor összegzi az eseményeket és rövid szóbeli visszajelzést adhat a résztvevők számára, bár a szóbeli visszajelzés soha nem helyettesítheti a kötelező írásos összefoglalót. A zárást követően a szervezők írásos dokumentumot készítenek, amely tartalmazza az események időrendjét, a játékosok észrevételeit és minden olyan adatot, amely az értékeléshez szükséges. Ez a dokumentum az értékelési szakasz kiindulópontja.

A gyakorlat teljes időtartama alatt felmerülő változásokat, eltéréseket vagy rendkívüli eseményeket jegyzőkönyvben kell rögzíteni, beleértve a szabályoktól való indokolt eltéréseket is. A gyakorlat során vezetett naplók és jegyzőkönyvek nem módosíthatók utólag. Ha

kiegészítésre van szükség, azt csak külön megjegyzéssel lehet feltüntetni. Ez a követelmény biztosítja, hogy a gyakorlat minden lépése rekonstruálható, ellenőrizhető és hiteles maradjon.

A gyakorlat lefolytatása így egyszerre biztosítja a valósághű szimulációt és az objektív, átlátható vizsgálat feltételeit, miközben a szerepök következetes elválasztása garantálja, hogy az eredmények megbízható alapot jelentsenek a szervezeti fejlesztéshez és a későbbi értékelésekhez.

Dokumentálás és értékelés

A kiberbiztonsági gyakorlat valódi értéke nem pusztán a szimuláció végrehajtásában, hanem a tapasztalatok rendszerezett feldolgozásában és dokumentálásában rejlik. A dokumentálás és az értékelés feladata, hogy a szervezet teljes képet kapjon reagálási képességeiről, a gyakorlat során feltárt gyengeségekről és azokról a fejlesztési lépésekről, amelyek szükségesek a kiberbiztonsági érettség növeléséhez. Ez a folyamat biztosítja a visszakövethetőséget és a tanulási ciklus lezárását, valamint lehetővé teszi a jogszabályi megfelelés későbbi igazolását.

A gyakorlat során vezetett naplók, jegyzőkönyvek és eseménylisták képezik az értékelés alapját. Ezekben a dokumentumokban részletesen rögzíteni kell az eseményeket, a játékosok döntéseit, az alkalmazott kommunikációs lépéseket és azokat a problémákat vagy elakadási pontokat, amelyek a gyakorlat közben felmerültek.

A gyakorlat lezárását követően a szervezetnek harminc napon belül írásos értékelő beszámolót kell készítenie, amelyet meg kell küldeni az NKI részére a hunex@nki.gov.hu címre. A beszámolóban áttekinthető módon kell tartalmaznia a gyakorlat céljait és kiinduló helyzetét, a forgatókönyvet és a résztvevői szerepköröket, az események időrendjét, az észlelt hiányosságokat és a válaszlépések hatékonyságának értékelését. Az értékelő dokumentumban fel kell tüntetni a fejlesztési javaslatokat és azokat az intézkedési irányokat, amelyek alapján a szervezet növelni tudja ellenállóképességét.

Az értékelés során vizsgálni kell, hogy a reagálási idők megfeleltek-e a szervezet elvárásainak, hogy a döntéshozatal folyamata megfelelően dokumentált és követhető volt-e, hogy a kommunikáció pontosan és gyorsan zajlott-e, valamint, hogy az incidenskezelési lépések összhangban voltak-e a szervezet szabályzataival és szabványos gyakorlataival. Elemezni kell továbbá a technikai és szervezeti intézkedések hatékonyságát és a szervezeti egységek közötti koordináció minőségét, mivel ezek alapvetően befolyásolják a szervezet reagálási képességét egy valós incidens esetén.

A résztvevők visszajelzése a folyamat szerves része. A játékos csapat számára írásos visszajelzést kell biztosítani, amelyben a szervezet összefoglalja a gyakorlat eredményeit, kiemeli az erősségeket és azokat a területeket, ahol fejlesztésre van szükség. Ez a kommunikációs lépés a tanulási és fejlesztési folyamat kulcseleme is, amely elősegíti a gyakorlat tapasztalatainak beépülését a mindennapi működésbe.

A gyakorlat megfelelőségét a Központ értékeli a benyújtott beszámoló és a rendelkezésre álló dokumentáció alapján. Az értékelés során az NKI jogosult megállapítani az esetleges hiányosságokat, valamint vizsgálni, hogy a gyakorlat végrehajtása és az abból levont következtetések összhangban állnak-e a jogszabályi és szakmai elvárásokkal. Amennyiben az értékelés eredménye indokolja, az NKI kezdeményezheti a védelmi intézkedések módosítását,

további fejlesztési lépések megtételét, illetve szükség esetén a gyakorlat megismétlését. Ez a felügyeleti mechanizmus biztosítja, hogy a gyakorlat valóban hozzájáruljon a szervezet kiberbiztonsági érettségének mérhető és ellenőrizhető növeléséhez.

A dokumentálás és értékelés így nem egy adminisztratív feladat, hanem a kiberbiztonsági képességek fejlesztésének és az elszámoltathatóság biztosításának alapja. A részletes írásos rögzítés és az elhatárolt értékelési folyamat garantálja, hogy a gyakorlatból valós, mérhető és ellenőrizhető tanulságok szülessenek, amelyek hosszú távon is erősítik a szervezet felkészültségét.

Utókövetés

A kiberbiztonsági gyakorlat nem ér véget a szcenárió lezárásával és az értékelő beszámoló elkészítésével. A valódi értéket az jelenti, ha a szervezet képes a tapasztalatokat feldolgozni, a feltárt hiányosságokat kijavítani, és az eredményeket tartósan beépíteni a mindennapi működésébe. Az utókövetési szakasz feladata a folyamatos fejlődés biztosítása, az intézkedések dokumentált végrehajtása és a szervezet kiberbiztonsági ellenálló képességének hosszú távú növelése. A szervezetnek felül kell vizsgálnia és módosítania szükséges az információbiztonsági szabályzatát a gyakorlat alkalmával feltárt hiányosságok alapján.

Az utókövetési folyamat első lépése a javító intézkedési terv elkészítése. A tervet az értékelő jelentés megállapításai alapján kell összeállítani, minden esetben írásban. A dokumentumnak egyértelműen tartalmaznia kell a feltárt hiányosságokat, a javasolt fejlesztési vagy korrekciós lépéseket, a felelősöket, a végrehajtási határidőket és a várt eredményeket. A javító intézkedési terv elkészítéséért felelős személy nem lehet az értékelést végző személyével, ez biztosítja az elhatárolás követelményét és az értékelési folyamat függetlenségét. A tervet a szervezet vezetésének írásban kell jóváhagynia, és meg kell határozni a végrehajtás nyomon követésének rendjét.

A végrehajtás során minden lépést részletesen dokumentálni kell. A dokumentációnak tartalmaznia kell a teljesítés dátumát, az alkalmazott megoldás leírását, a felelős személy visszajelzését és az ellenőrzés eredményét. A dokumentált bizonyítékok biztosítják a folyamat visszakövethetőségét és az elszámoltathatóságot, különösen hatósági ellenőrzés vagy belső audit esetén.

A végrehajtás előrehaladását rendszeresen értékelni kell. A szervezet vezetése és az elektronikus információs rendszer biztonságáért felelős személy legalább negyedévente köteles írásos státuszjelentést készíteni, amely áttekinti az elvégzett intézkedéseket, a még nyitott feladatokat és a szükséges módosításokat. A státuszjelentést az NKI részére meg kell küldeni a hunex@nki.gov.hu címre. Amennyiben a szervezet megítélése szerint a fejlesztések elérték céljukat, zárójelentést kell készíteni és azt szintén az NKI részére kell benyújtani, amely dokumentáltan rögzíti a javító lépések eredményességét.

Abban az esetben, ha az NKI az értékelő beszámoló vagy az utókövetési folyamat alapján úgy ítéli meg, hogy a hiányosságokat nem javították ki megfelelően vagy a hibák ismétlődnek, a szervezet kötelezhető a gyakorlat megismétlésére. A megismétlésről szóló kötelezést minden esetben írásban kell közölni. A szervezetnek ezt követően új, módosított intézkedési és gyakorlati tervet kell készítenie. A megismételt gyakorlat eredményeit önálló jelentésben kell dokumentálni, amely kiegészíti a korábbi dokumentációs láncolatot.

Az utókövetési folyamat minden elemét írásban kell rögzíteni. A javító intézkedési terv, a végrehajtás nyilvántartásai, a rendszeres státuszjelentések és a zárójelentések együttesen alkotják a kiberbiztonsági gyakorlat teljes dokumentációs keretrendszerét. Ez a keretrendszer átláthatóan mutatja be a szervezet fejlődési folyamatát, biztosítja a megfelelőség igazolhatóságát és hozzájárul a kiberbiztonsági kultúra folyamatos erősítéséhez.

A gyakorlat típusai

A kiberbiztonsági gyakorlatok többféle formában valósíthatók meg, attól függően, hogy a szervezet milyen célokat kíván elérni, milyen kockázati tényezőkre kíván reagálni, milyen erőforrások állnak rendelkezésére, valamint milyen alaptevékenységet lát el, és ebből következően milyen fenyegetettségi környezetben működik. A megfelelő gyakorlat típusának kiválasztása alapvetően meghatározza a gyakorlat eredményességét, ezért minden esetben írásban kell rögzíteni, hogy a választott forma miként illeszkedik a szervezet felkészültségi szintjéhez, célrendszeréhez és működési sajátosságaihoz. A típus kiválasztásakor mindig figyelembe kell venni az elhatárolás követelményét, vagyis azt, hogy a tervezés, a lebonyolítás, az értékelés és a játékos részvétel szerepei nem fedhetik egymást. Ezt a követelményt a dokumentációban egyértelműen fel kell tüntetni. Amennyiben a gyakorlat külső fél bevonásával történik, az együttműködés feltételeit és a felelősségi határokat írásos megállapodásban kell rögzíteni.

Asztali gyakorlat

Az asztali gyakorlat célja a döntéshozatali és kommunikációs folyamatok vizsgálata technikai beavatkozás nélkül. A résztvevők egy előre kidolgozott kiberbiztonsági helyzetet elemeznek, és közösen határozzák meg a szükséges válaszlépéseket. Az asztali gyakorlat előnye, hogy viszonylag alacsony erőforrásigény mellett tesztelhetők a vezetői döntések, az incidenskezelési eljárások és a szervezeten belüli koordináció. A forgatókönyvet részletesen előre el kell készíteni, és a gyakorlat során minden döntést, felvetést és javaslatot írásban kell rögzíteni.

Technikai gyakorlat

A technikai gyakorlat a szervezet informatikai rendszereinek valós támadásokat megközelítő szimulációját jelenti. Célja a detektálási, reagálási és helyreállítási képességek vizsgálata. A gyakorlat során valós vagy elkülönített tesztkörnyezetben hajtanak végre támadási szimulációkat, amelyekre a technikai csapatok valós incidenskezelési folyamatok szerint reagálnak. A lebonyolítás részleteit, a használt eszközöket, az időzítést és a biztonsági határvonalakat részletes technikai tervben kell rögzíteni. A gyakorlat során a támadások, észlelések és reagálások minden lépését időbélyeggel ellátott logokban kell rögzíteni. A gyakorlat végén részletes technikai értékelést kell készíteni, amely tartalmazza a detektálási időket, a reagálási lépéseket és azok hatékonyságának elemzését.

Vegyes gyakorlat

A vegyes gyakorlat az asztali és technikai elemeket ötvözi, és egyszerre vizsgálja a vezetői döntéshozatalt, a kommunikációt és a technikai reagálást. Ez a típus adja a legátfogóbb visszajelzést a szervezet kiberbiztonsági működéséről, ezért kiemelten alkalmas a teljes reagálási lánc elemzésére. A vegyes gyakorlat nagyobb komplexitása miatt különösen fontos a

szerepkörök és felelőségek egyértelmű írásos szétválasztása. A lebonyolítás során minden eseményt, kommunikációt és döntést részletesen dokumentálni kell a gyakorlat naplójában. A gyakorlat lezárása után külön értékelő jegyzőkönyvet kell készíteni, amely mind a technikai, mind a vezetői tapasztalatokat rögzíti. Az értékelés során a technikai és szervezeti eredményeket össze kell vetni, hogy komplex képet lehessen adni a szervezet reagálóképességéről. A végleges értékelő dokumentum tartalmazza a fejlesztési javaslatokat, amelyek az intézkedési terv elkészítésének alapját képezik.

Dokumentálási követelmények minden típus esetében

A gyakorlat típusától függetlenül minden esetben kötelező a forgatókönyv és a célkitűzések írásos rögzítése, a szerepkörök és felelőségek elhatárolása, az események és döntések időbélyeges dokumentálása, valamint a lezáró értékelés és visszajelzések részletes írásos összegzése. Minden dokumentumot a szervezet iratkezelési rendje szerint kell megőrizni, hogy biztosított legyen a visszakövethetőség, az objektivitás és az ellenőrizhetőség. Ezek a követelmények garantálják, hogy a gyakorlat eredményei megbízható alapot jelentsenek a szervezet fejlesztéséhez és megfelelőségének igazolásához.

Minimum követelmények

A kiberbiztonsági gyakorlatok csak akkor járulnak hozzá érdemben a szervezetek ellenálló képességének növeléséhez, ha megfelelnek bizonyos alapvető elvárásoknak. Ezek a minimumfeltételek biztosítják, hogy a gyakorlat ne pusztán formai kötelezettség legyen, hanem olyan folyamat, amely valós fejlődést, mérhető eredményeket és ellenőrizhető működést eredményez. A követelmények betartása minden szervezet számára kötelező, és a gyakorlat teljes dokumentációs láncolatában írásban igazolni kell.

Rendszeresség és kötelezettség

A szervezeteknek legalább két évente részt kell venniük egy kiberbiztonsági gyakorlaton, amely lehet önálló, cégcsoportos vagy az NKI által szervezett gyakorlat, és amely biztosítja a felkészültség folyamatos fenntartását és fejlesztését. Az NKI által elrendelt vagy hatósági előírásokon alapuló gyakorlatokon való részvétel minden érintett szervezet számára kötelező. A részvétel és a végrehajtás megtörténtét írásos formában kell dokumentálni, amely a későbbi ellenőrzések alapjául szolgál.

Cégcsoporthoz tartozó szervezetek dönthetnek úgy, hogy a gyakorlatot közös szervezésben és összehangolt módon valósítják meg, amennyiben ez összhangban áll működési struktúrájukkal és kockázati környezetükkel. Ilyen esetben is biztosítani kell, hogy az egyes szervezetek saját rendszereire, folyamataira és felelőségi viszonyaira vonatkozó értékelés elkülöníthető és dokumentált legyen, valamint hogy a részvétel és a végrehajtás igazolása szervezetenként egyértelműen megtörténjen.

Elhatárolás követelménye

A gyakorlat lebonyolításában részt vevő és a gyakorlaton játékosként részt vevő személyek nem lehetnek azonosak, a két szerepkör között nem lehet átfedés. A tervezés, a szervezés, az értékelés és az utókövetés feladatait el kell különíteni a ténylegesen gyakorlatozó résztvevőktől,

és ezt a szerepmegosztást a gyakorlat megkezdése előtt írásban rögzíteni kell. A dokumentációnak egyértelműen tartalmaznia kell a felelősségi köröket, ezzel biztosítva az objektivitást és az értékelés hitelességét. Nagy jelentőségű gyakorlat esetén indokolt lehet az értékelés és az utókövetés független, akár külső szervezet általi elvégzése.

Írásbeliség és dokumentáció

Minden gyakorlatnak részletes, írásban rögzített tervvel kell rendelkeznie, amely tartalmazza a célokat, a scenáriót, a szerepköröket, a felelősségi határokat és a végrehajtási szabályokat. A lebonyolítás során keletkező naplók, jegyzőkönyvek, döntési listák, logok és visszajelzések kötelező mellékletei az értékelési folyamatnak. A dokumentumokat időbélyeggel és hitelesítéssel kell ellátni, és utólag nem módosíthatók, csak kiegészítő megjegyzésekkel egészíthetők ki. Az értékelés, az utókövetés és a javító intézkedések végrehajtása minden esetben írásos formában történjen, hogy biztosított legyen a folyamat visszakövethetősége és auditálhatósága. Az írásbeliség nem formai követelmény, hanem a gyakorlat érvényességének alapfeltétele.

Valóságosság és arányosság

A forgatókönyveket a szervezet valós kockázataihoz, működési sajátosságaihoz és erőforrásaihoz kell igazítani. A gyakorlatnak valóságghűen kell modelleznie a kiberfenyegetéseket, ugyanakkor nem veszélyeztetheti a szervezet folyamatos működését, és nem okozhat aránytalan terhelést a résztvevők számára. A tervezési dokumentumokban írásban kell rögzíteni a szimulált események várható hatásait, valamint azokat a kockázatcsökkentő intézkedéseket, amelyek biztosítják, hogy a gyakorlat biztonságos keretek között maradjon. Az arányosság követelménye garantálja, hogy a gyakorlat valós helyzeteket tükröz, de nem veszélyezteti a szervezet működőképességét.

Részvétel és együttműködés

A gyakorlat során be kell vonni az elektronikus információs rendszer biztonságáért felelős személyt, valamint minden releváns szervezeti egységet, így különösen az informatikai, jogi és kommunikációs területet, továbbá a vezetést. Amennyiben a gyakorlat jellege indokolja, külső partnereket, szolgáltatókat vagy hatóságokat is be kell vonni. A résztvevők körét és szerepköreit előzetesen, írásban kell rögzíteni. A lebonyolítás során biztosítani kell a koordinált együttműködést, ugyanakkor fenn kell tartani az elhatárolást az értékelő funkciótól. Minden kommunikációról, döntésről és együttműködésről részletes írásos nyilvántartást kell vezetni, amely később az értékelés és az utókövetés alapját képezi.

Átláthatóság és ellenőrizhetőség

A gyakorlat teljes folyamatát átlátható módon kell vezetni és dokumentálni, a tervezéstől az utókövetés lezárásáig. Minden döntésről, változtatásról vagy eltérésről részletes jegyzőkönyvet kell készíteni. Az NKI és más illetékes hatóság jogosult a teljes dokumentáció utólagos ellenőrzésére, ezért valamennyi iratot, jegyzőkönyvet és beszámolót legalább öt évig meg kell őrizni. Az átlátható és dokumentált működés biztosítja, hogy a gyakorlat ellenőrizhető, auditálható és visszakövethető legyen, függetlenül attól, hogy belső kezdeményezésre vagy hatósági kötelezés alapján valósult meg.

A gyakorlatokkal kapcsolatos minden hivatalos kommunikáció az NKI kijelölt elérhetőségén keresztül történik, amelynek címe hunex@nki.gov.hu. Ezen a címen lehet jelezni a gyakorlat tervezése során felmerülő kérdéseket, például a forgatókönyv értelmezésével, a szerepkörök tisztázásával vagy a dokumentációs követelményekkel kapcsolatban. Ugyanitt lehet bejelenteni

a lebonyolítás közben felmerülő technikai vagy szervezési problémákat, ideértve a szimuláció során tapasztalt informatikai hibákat, az együttműködéssel kapcsolatos akadályokat és minden olyan körülményt, amely a gyakorlat előrehaladását vagy biztonságát érintheti. A gyakorlat lezárását követően erre a címre kell megküldeni a harminc napon belül elkészített értékelő beszámolót, a kiegészítő dokumentumokat és az utókövetési iratokat. Az NKI kijelölt elérhetősége így a kérdések, problémabejelentések, értékelések, egyeztetések és hivatalos beadványok egységes kommunikációs felülete, amely biztosítja a teljes folyamat átláthatóságát és visszakövethetőségét.