VAN-E ÉLET AZ AUDIT UTÁN? Mire figyeljünk, hogy a következő auditon is átmenjünk? Hogyan alakítsunk ki hosszú távon fenntartható IBIR-t?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/24

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.26	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A NIS2-nek megfelelő kiberbiztonsági megfelelés valójában nem „audit-projekt”, hanem folyamatos feladat, ami biztosítja a szervezet biztonságos működtetését. A fenntartható IBIR (Információbiztonság Irányítási Rendszer) ezért akkor működik jól, ha a szervezet olyan szabályozási és működési, folyamatokat, dokumentációs rendet alakít ki, amelyet valóban be is tud tartani, és amely a mindennapi üzemeltetésben, fejlesztésben, beszerzésben, valamint az emberi működésben (képzés, felelősségek, kontrollok) szinte „magától működik”, nem terheli plusz feladatokkal a szervezetet.

A 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás és a konkrét adminisztratív–logikai–fizikai intézkedések oldaláról adja meg a megfelelés gerincét. A rendelet kifejezetten kimondja, hogy a szervezetre a rendelet szerint kidolgozott szabályzatokban rögzített védelmi intézkedések az irányadók, ugyanakkor indokolt lehet eltérés, esetleg kiegészítő, illetve helyettesítő védelmi intézkedésekkel, kockázatelemzéssel alátámasztva. Ennek gyakorlati üzenete: a papíron tökéletes, de valójában nem működtetett kontrollrendszer nem megfelelő, ellenben egy működő, mért és indokolt eltérés, a megfelelő kiegészítéssel, elemzéssel a rendeleti logika megfelelőségébe illeszthető.

A szervezet komoly hibát követ el, ha a következő auditra az audit előtti néhány hétben kezd el felkészülni, mivel annak már egyértelműen vizsgálati hatóköre lesz az is, hogy a most megalkotott rendszer valójában működik-e. Nyilvánvaló, hogy a hetek alatt esetlegesen „legyártott” audit bizonyítékok nem fogják alátámasztani a megfelelő működést. Elvárás, hogy a korábban megállapított esetleges eltérések is beépüljenek a kockázatkezelésbe és ezen keresztül a folyamatokba, valamint hogy a jól működő kontrollok dokumentáltan, igazolhatóan működjenek, az auditok közötti időszakokban is.

A NIS2 hazai megfelelésében az „audit utáni élet” valójában az IBIR valódi élete: az audit megállapítások beépítése a folyamatokba, a kontrollok folyamatos működtetése, és a szabályozási rend karbantartása.

A következő audit sikerének legbiztosabb módja az, ha a szervezet nem auditokra készül, hanem folyamatszinten működteti az információbiztonság irányítási rendszert. Ezzel a megfelelés nem kampányjellegű teher, hanem olyan működési rutin lesz, amely egyszerre javítja a biztonságot és csökkenti a következő audit kockázatát.

2. LEGFONTOSABB TEVÉKENYSÉGEK

2.1 Az auditjelentés és a megállapítások feldolgozása, bevezetése a kockázatkezelésbe

Az audit utáni első kritikus lépés a jelentés és az audit folyamat „adminisztratív lezárása” helyett a megállapítások működési szintű feldolgozása. Célszerű a megállapításokat egységes struktúrában, a szervezet által végzett kockázatelemzésnek megfelelően rögzíteni. A kockázatelemzésnek és kezelésnek továbbra is alkalmasnak kell lennie arra, hogy később auditbizonyítékként is bemutatható legyen az, hogy mikor, ki, mit döntött, milyen kockázati indok alapján és milyen ellenőrzési módszerrel.

A vezetés feladata, hogy a megállapításokhoz felelőst, erőforrást és határidőt rendeljen. A megállapítások jelentős része várhatóan nem tisztán informatikai jellegű. Tipikusan érintheti a beszerzést, beszállítói szerződéseket, HR-folyamatokat, változáskezelést, üzletmenet-folytonosságot. Emiatt a „kijavítás” nem lehet kizárólag IT- vagy IT biztonsági szervezeti egység feladata; a felelősök kijelölésekor a folyamatgazdákat kell elsődlegesen megcélozni, továbbá a feladatok végrehajtásába be kell vonni az érintett területeket.

A megállapítások bevezetése a kockázatelemzésbe akkor hatékony, ha minden megállapítás kap egy kockázati bejegyzést, az elemzés módszertana szerint. Tartalma:

- mi a fenyegetés/gyengeség, mi az érintett eszköz és üzleti folyamat,
- mekkora a hatás valószínűsége és következménye,
- milyen meglévő kontrollok csökkentik,
- és mi a kockázatkezelési döntés (elfogadás, csökkentés, átruházás, megszüntetés).

Nem kizárt, hogy a szervezet bizonyos eltéréseket nem javít (felvállalja a kockázatot), azonban ebben az esetben ezt indoklással, elemzéssel kell alátámasztani.

Akár célszerű lehet külön az auditmegállapításokból javító intézkedési tervet készíteni, amelynek része a hatékonyságmérés is. A következő auditon várhatóan (az újabb vizsgált EIR-ek mellett) jellemző kérdés lesz, hogy megoldódott-e az adott probléma? Erre a végrehajtás bizonyítékai: naplók, jegyzőkönyvek, változáskezelési ticketek, képzési naplók, tesztjegyzőkönyvek, adhatnak hiteles választ.

2.2 Kockázatelemzés és kockázatkezelés folyamatos végrehajtása

A fenntartható IBIR egyik alappillére a folyamatos kockázatmenedzsment, amely nem éves „egyszeri gyakorlat”, hanem folyamatos, üzleti és technikai változásokhoz kötött működés. A rendeleti környezet alapvetően a kockázati logikára támaszkodik, ezért a kockázatkezelésnek módszertanilag következetesnek kell lennie.

A szervezetnek szükséges rögzíteni a kockázatmenedzsment stratégiáját, amely tartalmazza, hogy hogyan történik az azonosítás, értékelés, kezelés és felügyelet. A 7/2024 MK rendelet kifejezetten elvárásként nevesítik a szerepkörök, felelősségek, hatáskörök, kockázatmenedzsment stratégia és a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére szolgáló biztonságfelügyeleti stratégia dokumentálását. Ez a gyakorlatban például azt jelenti, hogy legyenek kijelölt felelősök, határidők, illetve legyenek meghatározva a pontos feladatok (javítás, csökkentés), valamint ami mindennél fontosabb: legyenek a szükséges erőforrások hozzárendelve a feladathoz.

A kockázatkezelésben tipikus, „jó gyakorlat” megoldás, ha negyedéves rendszerességgel végez a szervezet kockázati felülvizsgálati fázisokat / státuszokat, valamint szükség esetén eseményvezérelt módon, például súlyos sérülékenységek megjelenése, jelentős incidens bekövetkezése, nagyobb architekturális módosítás, új rendszer bevezetése, vagy hasonló esemény bekövetkezésekor. A kockázatkezelési döntéseknek minden esetben vezetői jóváhagyással kell rendelkezniük, különösen akkor, ha a szervezet kockázat felvállalást választ.

A kockázatkezelést érdemes összekötni mérőszámokkal. Ilyenek lehetnek például:

- sérülékenységek javítási ideje;

- backup visszaállítási tesztek ideje, sikeressége;
- jogosultsági felülvizsgálatok lefedettsége;
- incidensek átlagos detektálási és elhárítási ideje.

Ezek a KPI-k nem „extra adminisztrációk”, hanem a vezetői kontroll részei, és a következő auditon erős bizonyítékot adnak a kockázatkezelés működtetésre.

2.3 Szabályozási környezet felülvizsgálata és naprakészen tartása

A szabályozási rend fenntarthatóságának alaptétele, hogy csak olyan követelményeket szabad belső szabályzatként rögzíteni, amelyeket a szervezet ténylegesen képes betartani. A 7/2024 MK rendelet a védelmi intézkedéseket a szervezet saját szabályzataiban rögzített formában kéri számon; ez a gyakorlatban azt jelenti, hogy a szabályzatoknak tartalmazniuk kell a megfelelés szervezetre szabott megvalósítását.

Ha a szabályzat túl „ambiciózus” és túlontúl sok nyilvántartási, dokumentációs és / vagy technikai követelményt határoz meg, akkor annak betartása a szervezet számára megoldhatatlan lesz, ami viszont az auditon könnyen és gyorsan kiderül, így nem ez a jó irány a megfelelőséghez.

A szervezetnek célszerű szabályozási térképet (policy map) fenntartani, milyen szabályozási struktúrát használ, melyek a fő szabályzatok, melyek az eljárásrendek (melyik szinteket ki adja ki), melyek az átfogó szabályozási elemek és melyek a rendszerszintűek. Nagyon hasznos, ha a szervezet biztonsági felelőse (szervezeti egysége / felkészítője) akár olyan részletességig ismeri a környezetet, hogy le tudja írni, hogy melyik jogszabályi előírás melyik belső dokumentumban, melyik fejezetben teljesül. Ez nagyban segíti majd az auditálhatóságot.

A szabályozás mellett célszerű egy verziókövetési rendet is vezetni: melyik mikor volt utoljára felülvizsgálva, mi változott, milyen döntések születettek. Fontos annak a figyelése is, hogy esetlegesen változik-e a jogszabályi környezet, mert ha igen, akkor azokat is le kell követni (ez a kétéves audit ciklusokban előfordulhat).

A szabályozások felülvizsgálata nem csak jogszabályi kérdés / előírás. A belső szabályzatoknak követniük kell a szervezet architektúráját és működését, például bármi technikai változás esetén: felhőhasználat, külső szolgáltatók, új identitáskezelési megoldások, új naplógyűjtés.

A szabályozás és a valós működés közötti „rés” a leggyakoribb auditkockázat: van szabály, de nincs, vagy nem úgy működik a végrehajtás, vagy van ugyan folyamat, de nincs dokumentált módon szabályozott folyamat, eljárás.

A szervezet számára célszerű éves felülvizsgálatokat bevezetni, a szabályzatok, kockázatok, kontrollhatékonyság és auditmegállapítások áttekintésére. Ez egyszerre felel meg a jó irányítási gyakorlatnak és auditbizonyítékot is ad arra, hogy az IBIR nem „dokumentumhalmaz”, hanem egy valóban működő rendszer.

2.4 Fő folyamatok dokumentált működtetése

A fenntartható IBIR a folyamatok stabil, dokumentált működésén áll vagy bukik. Ezek közül – kissé önkényesen – a következőket emelnénk ki: jogosultság- és hozzáférés- kezelés; konfiguráció- és változáskezelés; sérülékenységek kezelése; frissítések / karbantartások végzése; naplózási területek;

mentések és kapcsolódó folyamatok (és technikai megvalósítás); BCP/DRP tervek megléte, megfelelősége, tesztelése

A jogosultságkezelésben a szervezetnek célszerű szerepköralapú modellt kialakítania. A folyamatnak illeszkednie kell a HR folyamatokhoz is (pl.: ki- és belépés, áthelyezések). A munkatársaknak és vezetőknek egyértelműen tudniuk kell, hogy melyik rendszerben ki hagy jóvá jogosultságot (üzleti felelős), ki valósítja meg (IT), és ki ellenőriz (információbiztonság / belső ellenőrzés / üzleti terület vezetése). Erős auditbizonyíték a rendszeres (pl. negyedéves vagy féléves, de legfeljebb éves) jogosultsági felülvizsgálat, amelynek kimenete tényleges visszavonásokat és korrekciókat is tartalmaz. A rendszeres felülvizsgálatok mellett kezelni kell az egyedi eseteket is (pl.: külső munkatársak, szerződéses partnerek). Problémás terület lehet a technikai hozzáférések kezelése is, ezzel is kell foglalkozni az auditok közötti időszakokban.

Konfigurációkezelés és változáskezelés esetén tipikus elvárás, hogy a szervezet a módosítások előtt biztonsági hatásvizsgálatot végezzen:

- milyen kockázatok merülhetnek fel,
- változik-e a naplózás, érinti-e az azonosítást,
- sérül-e a szegmentáció,
- módosulnak-e a mentési és helyreállítási paraméterek.

A változásokhoz kezeléséhez, vizsgálatához és jóváhagyásához célszerű egységes jegyrendszert (ticketing) használni, amelyben szerepel a kockázati értékelés, egyértelmű a felelős jóváhagyás.

A frissítések és karbantartás területén a fenntarthatóságot a jó „ütemezési gyakorlat” és a rendszeresség adja meg (akár SLA-k). A tervezett karbantartások, illetve a meghatározott és (például ticketing rendszerben) dokumentált folyamatok biztosítják a megfelelőséget. A frissítések során nem elvárás, hogy minél gyorsabban kerüljenek végrehajtásra, még a biztonsági frissítések esetén sem. Az az elvárás, hogy a sérülékenységek kockázat arányos módon és ésszerű időn belül kerüljenek javításra.

A naplózás témakörében jó gyakorlat a központosított naplógyűjtés, lehetőleg automatikus elemzés és riasztás, valamint a riasztások kezelésének dokumentált rendje (kivizsgálási lépések, döntési pontok, lezárási kritériumok).

A biztonsági mentések (offline is), nem csak az audit, hanem a szervezet fennmaradása szempontjából is kiemelt fontosságúak. Ennek megfelelően a mentések tesztelése, visszatöltése a közelgő audittól függetlenül is kötelezően végrehajtandó feladat. Hasonló terület a BCP és DRP tervek megléte, megfelelősége, amelyeknél a jó auditálhatóság kulcsa a tesztelés. A szervezetnek célszerű rendszeres (pl. féléves, maximum éves) visszaállítási teszteket végeznie, BCP / DRP gyakorlatot tartania legalább a kritikus szolgáltatásokra. A teszteknek mérőszámokkal és a tanulságok levonásával kell zárulniuk (RTO/RPO teljesülés, hiányosságok, javító intézkedések), és ezeknek be kell épülniük a kockázatkezelésbe, valamint a tervekbe.

2.5 Sebezhetőségek és sérülékenységek kezelése

Gyakori auditmegállapítás, hogy van eseti sérülékenységszkennelés, de nincs állandó folyamat, nyilvántartás, nincs kockázatalapú priorizálás, vagy a javítások nem követhetőek végig dokumentált módon, biztonsági hatásvizsgálattal alátámasztva.

A szervezetnek célszerű rögzítenie, milyen gyakorisággal történik sérülékenység elemzés (ismert sérülékenységek vizsgálata), illetve sérülékenységvizsgálat / vagy behatolás vizsgálat (pl.: belső, külső, infrastruktúra, alkalmazás, …), mely rendszerek kritikusak, és milyen javítási célidők kapcsolódnak a különböző súlyosságú sérülékenységekhez. A priorizálásban célszerű figyelembe venni az üzleti folyamat kritikusságát valamint a sebezhetőség típusát (pl. egy távolról kihasználható hiba esetén az internet felől elérhető komponensek javítását gyorsan el kell végezni, ha nem alkalmazunk más védelmi intézkedést).

Amennyiben egy sérülékenység javítása nem lehetséges (pl. legacy rendszer, technikai függés, stb.), akkor van mód kiegészítő védelmi kontrollokat alkalmazni, de ezeknek a megfelelő kockázatkezelési folyamaton végig kell mennie, valamint ezeket megfelelően dokumentálni kell (pl.: szegmentáció, hozzáférés-korlátozás, szűrés hálózat határán, alkalmazásszintű védelem, fokozott monitorozás). Ebben az esetben nem szabad később sem megfeledkezni arról, hogy az alap kockázat megmaradt, ami a kiegészítő védelmi intézkedés kiesése esetén védtelenül maradhat (pl.: egy alkalmazáshiba a tűzfal szűrés kiesése esetén).

2.6 IT-rendszerek módosításakor a szükséges dokumentációk felülvizsgálata és módosítása

Az IBIR egyik tipikus gyenge pontja, hogy az IT változik, a dokumentáció viszont lemarad. A fenntartható modellben a dokumentáció frissítése nem külön feladat, hanem a változáskezelés kötelező kimenete. Célszerű a változás részeként kötelezően megjelölni (pl.: a jegykezelő rendszerben), milyen dokumentumokat érint a módosítás (pl.: architektúra leírás, hozzáférések, naplózási terv, mentési terv, BCP/DRP, üzemeltetési eljárások).

Érdemes a „minimális szükséges dokumentáció” elvét alkalmazni: ne legyen túl sok, párhuzamosan karbantartandó leírás, mert az gyorsan inkonzisztenssé válik. Jobb néhány, jól definiált, és verziózott dokumentumot fenntartani, amelyekre a kontrollok és auditbizonyítékok is visszahivatkoznak.

Az alkalmazás gazda és az üzemeltetés feladata, hogy a rendszerleírás és a kapcsolódó dokumentáció naprakész legyen. Az információbiztonsági felelős feladata, hogy a változás biztonsági hatásvizsgálata megtörténjen, és ha szükséges, kockázati bejegyzés készüljön. Az üzemeltetés feladata, hogy a változás utáni ellenőrzések (monitoring, loggyűjtés, mentés, hozzáférések kezelése) ténylegesen megtörténjenek és dokumentáltak legyenek.

A dokumentációfrissítések auditbizonyítékait is célszerű a változásokhoz kapcsolódó ticketekben tárolni. A következő auditon ez gyorsan bizonyítja a rendszer-szintű kontrollok működését.

2.7 Képzések rendszeres elvégzése meghatározott szerepkörökben

A szerepalapú és a NIS2 által meghatározott témájú képzések elvégzése alapvető és könnyen elvégezhető feladat. A könnyű megvalósíthatóság mellett egy alapvető audit megfelelőség, így ezt nem érdemes kihagyni a tevékenységek közül. Nem beszélve arról, hogy a mai kiberbiztonsági helyzetben igen komoly pozitív hatással van a szervezet biztonságára a felhasználók jó szintű biztonságtudatossága.

A munkatársak szintjén a minimum az, hogy az alapvető fenyegetések (pl.: adathalászat, jelszóhasználat, eszközvédelem, incidensjelentés) legyenek oktatva. A vezetők esetében célszerű a felelősségi és döntési pontokra fókuszálni: kockázatelfogadás, beszállítói döntések, BCP / DRP döntések meghozása és gyakorlatok támogatása.

A műszaki, technikai munkatársak számára célzott, szakértői képzések javasoltak.

Célszerű minden oktatást, képzést rövid tesztekkel, szimulációkkal zárni, így célzott visszaméréssel igazolni a hatékonyságot. A képzési hiányosságokat (lemaradás, sikertelen vizsga) javasolt kockázatként kezelni, és vezetői szinten nyomon követni.

2.8 Incidensek dokumentált kezelése, nyilvántartás és tanulságok levonása

Az incidenskezelési eljárásnak ki kell térnie az észlelésre, bejelentésre, triázsra, incidens kezelésére, elhárításra, helyreállításra és a kommunikációra – mind az érintettek (esetleg ügyfelek, partnerek), mind a hatóság(ok) irányába. Emellett szükséges incidens-nyilvántartás vezetése (körülbelül ezzel a tartalommal: mi történt, mikor, hogyan, érintett rendszer(ek), érintett adat(ok), mi volt a hatás, mi volt a fő ok, megoldás, milyen intézkedések történtek (kommunikáció is), javító intézkedések, hogyan előzhető meg, levont tanulságok).

Ezt mindenképpen szükséges vezetni, mivel a mai világban nem életszerű, hogy két éven keresztül semmilyen incidens nem történik.

A munkatársak feladata az, hogy tudják: mit és kinek kell jelezni ha incidenst észlel. A vezetők feladata, hogy az eszkalációs rend működjön, és kritikus helyzetben gyors döntések szülessenek (rendszerleválasztás, szolgáltatás-korlátozás / leállítás, harmadik felek bevonása, stb.). A technikai felelősök feladata, hogy az eset műszaki kivizsgálása, a bizonyítékok feltárása és megőrzése (logok, mentések) és a helyreállítás kontrollált legyen.

A tanulságok levonása (lessons learned) szükséges, és be kell épülnie a kontrollrendszerbe. Célszerű minden jelentősebb incidens után javító intézkedési tervet készíteni, és azt a kockázatkezelésben rögzíteni.

Az incidenskezelés megfelelő auditbizonyítéka manapság nem az, hogy „van eljárás”, hanem az, hogy léteznek lezárt incidensjegyek, kivizsgálási jegyzőkönyvek, és mérhetően javul a detektálás és reagálás. A naplózás (gyűjtés és elemzés), valamint a monitorozás fejlettsége (riasztások, kivizsgálási lépések) itt közvetlenül visszaköszönhetnek.

2.9 Beszállítói és szolgáltatói kockázatok kezelése

A NIS2-érintett szervezeteknél az ellátási lánc gyakran a legnagyobb kockázati felület, ennek kezelése ráadásul újdonság a korábbi előírásokhoz képest. Sok szervezet most találkozik először ezzel a témával. Célszerű beszállítói osztályozást fenntartani, és ehhez biztonsági követelményrendszert kapcsolni (pl.: szerződéses SLA-k; incidensek kezelése; auditálási lehetőség; mentési, naplózási és hozzáférés kezelési eljárások).

Az IT mellett elsősorban beszerzés és jogi (compliance) terület felelőssége, hogy a kiberbiztonsági kikötések ténylegesen bekerüljenek a szerződésekbe. Az IT és információbiztonság felelőssége, hogy műszaki oldalon is megvalósuljanak a korlátozások: pl.: távoli hozzáférések, szegmentáció, minimális jogosultság, naplózás. A vezetés / üzlet felelőssége, hogy kritikus szolgáltatók esetén legyen exit terv és alternatíva.

Jó audit bizonyítéknak számít a beszállítói értékelési nyilvántartás, az éves felülvizsgálat, valamint a kritikus beszállítókhoz kapcsolt kockázati bejegyzések és kompenzáló kontrollok.

2.10 Belső ellenőrzés, önértékelés és kontrollhatékonyság

A kétévente ismétlődő audit mellé célszerű belső önellenőrzési mechanizmust bevezetni, ha a szervezet rendelkezik erre megfelelő erőforrással (pl.: belső ellenőrzési / compliance szervezeti egység): éves kontroll-önértékelés, célzott témavizsgálatok (jogosultságok, mentések, naplózás, sérülékenységek), valamint vezetői felülvizsgálatok. Ez segít abban, hogy a hiányosságok ne az auditon vagy az előtt derüljenek ki.

A 7/2024 MK rendelet szemlélete is a folyamatos felügyelet és a védelmi intézkedések hatékonyságának ellenőrzése felé mutat, ezért a belső kontrollmérés jól illeszkedik a rendelet logikájába. A belső ellenőrzés akkor fenntartható és hasznos, ha rövid, egyszerű témákkal dolgozik, és a megállapítások bekerülnek a kockázatkezelési folyamatba.