T Business

NIS2: A kiberbiztonság új korszakának hírnöke

Készen áll a változásra?

Connecting your world.

NIS2
Mit, miért és mikor?

Az európai kiberbiztonsági szabályozás forradalmi reformja, a NIS2 irányelv (Network and Information Security Directive), mely 2023. január 13-án lépett hatályba, és amelynek implementálása a hazai jogszabályi környezetbe a 2023. évi XXIII. törvénnyel történt meg. A 2023. évi XXIII. törvény helyébe 2025. január 1-jei hatállyal a jelenleg hatályos 2024. évi LXIX. törvény lépett. Készen áll arra, hogy megfeleljen az új előírásoknak?
A NIS2 szabályozás megértése és annak való megfelelés kulcsfontosságú. Útmutatónk a 2024. évi LXIX. törvény (Kibertan. törvény) bevezetésével kapcsolatos főbb elemeket összegzi, felvázolva a következő lépéseket, és bemutatva, hogyan segíthetünk szervezetének a teljes alkalmazkodási folyamat során. Ismerje meg a legfontosabb változásokat, és tudja meg, hogyan alkalmazkodhat hatékonyan!

A NIS2 célkitűzései

Kritikus infrastruktúra védelem:
A szabályozás megerősíti Magyarország létfontosságú szektorainak kiberbiztonságát, ezzel biztosítva a nemzetbiztonságot és a szolgáltatások folytonosságát.

Vállalati kiberképesség érettség növelés:
A törvény a magyar vállalatok széles körét vonja be a kiberbiztonsági követelmények hatálya alá, proaktív felkészülésre és a digitális ökoszisztéma ellenállóképességének növelésére ösztönözve őket.

Incidensjelentés és nemzeti reagálás:
A NIS2 szabályozás gyorsabb és pontosabb incidensjelentést ír elő, erősítve a nemzeti hatóságok valós idejű felderítési és összehangolt reagálási képességét Magyarországon.

Nemzetközi együttműködés és infómegosztás:
A szabályozás elősegíti a tagállamok közötti információcserét, erősítve ezzel Magyarország aktív részvételét az európai kiberbiztonsági hálózatban és a nemzetközi védekezésben.

A 2024. évi LXIX. törvény elsődleges **célja, hogy ellenállóbbá tegye Magyarország kritikus infrastruktúráját és alapvető szolgáltatásait a kiberfenyegetésekkel szemben.** Ennek érdekében a törvény:

· **Szigorúbb biztonsági követelményeket ír elő** az érintett hazai szervezetek számára, ezzel közvetlenül növelve azok kiberbiztonsági felkészültségét.
· **Hatékonyabb és gyorsabb incidensreagálást tesz kötelezővé**, ami lehetővé teszi a támadások okozta károk minimalizálását.
· **Támogatja a fenyegetésfelderítési információk megosztását a tagállamok között,** ezzel erősítve Magyarország aktív szerepét az európai kiberbiztonsági együttműködésben.

Mindezek eredményeként a NIS2 irányelv egységes és magasabb színvonalú információbiztonságot teremt az Európai Unióban, Magyarországon pedig a hazai jogszabályi környezetbe történő átültetéssel, valamint hozzájárulva az országos kiberbiztonsági helyzet általános javulásához és az európai digitális tér stabilitásához.

Felkészülés a NIS2-re:
Dátumok és Elvárások

A NIS2 irányelv céljainak eléréséhez, a sikeres vállalati felkészüléshez és a jogszabályi megfeleléshez elengedhetetlen a bevezetéshez kapcsolódó határidők és kötelezettségek pontos ismerete, valamint azok betartása.

Lejárt határidők (tájékoztató jelleggel):

- **2024. október 18.:** Szervezet osztályba sorolása és a megfelelő védelmi szint kialakítása.

- **2025. január 1.:** Új Kibertan. törvény hatályba lépése. Az újonnan érintetté váló cégeknek a tevékenység megkezdésétől számított 30 napjuk volt a bejelentkezésre.

- **2025. július 31.:** Az érintett szervezetek nyilvántartásba vételi kötelezettségének teljesítése a Szabályozott Tevékenységek Felügyeleti Hatóságánál (SZTFH).

- **2025. augusztus 31.:** A 2025. január 1. előtt már működő szervezeteknek eddig a dátumig kellett szerződést kötniük kiberbiztonsági auditorral, valamint igazolniuk kell a szerződéskötés teljesítését.

Aktuális és jövőbeli határidők (kiemelten fontos):

- **Díjfizetés:**
2026. március 31.: A kiberbiztonsági felügyeleti díj fizetési határideje (a 2/2025. SZTFH rendelet 6. §-a alapján).

- **Audit elvégzése:**
2026. június 30.: Az audit elvégzésének eredeti, 2025. december 31-i határideje az SZTFH rendelet késedelme miatt eltolódott. A 2025. január 1. előtt működő szervezeteknek az auditot 2026. június 30-ig kell elvégeztetniük.

Dinamikus határidők (folyamatosan érvényes):

- **120 nap (≈ 4 hónap):**
A 2024. évi LXIX. törvény szerint a nyilvántartásba vett szervezeteknek 120 napon belül (≈ 4 hónap) kell kiberbiztonsági auditorral szerződést kötniük. (Az SZTFH 2025. június 27-i tájékoztatása alapján a 2025. január 1. előtt már működő szervezetek számára ettől eltérően 2025. augusztus 31. volt a határidő az auditori szerződés megkötésére.)

- **24 óra:**
Az észleléstől számítva haladéktalanul, de legkésőbb ezen időn belül be kell jelenteni az incidenseket az SZTFH felé. Ha a teljes információ nem áll rendelkezésre 24 órán belül, akkor előzetes bejeletés tehető, amelyet legkésőbb 72 órán belül ki kell egészíteni és be kell nyújtani a részletesebb előzetes jelentést. Ez kiemelten fontos az incidenskezelés gyorsaságának szempontjából.

Ezeknek a határidőknek a betartása kulcsfontosságú a jogszabályi megfelelés és a vállalat kiberbiztonsági felkészültsége szempontjából.

Ellenőrizze, hogy a kiberbiztonsági törvény vonatkozik-e az Ön szervezetére! Kérje ingyenes konzultációnkat!

NIS2

Kik is az érintettek?

A NIS2 irányelv két fő kategóriába sorolja az érintett szervezeteket. Ez a besorolás a kockázat és a társadalmi hatás alapján történik, amely meghatározza az elvárt kiberbiztonsági intézkedések szintjét és az ellenőrzések gyakoriságát:

- **Alapvető szervezetek (Kiemelten kockázatos ágazatok):** Olyan szektorok és szervezetek tartoznak ide, amelyek szolgáltatásainak megakadása **súlyos zavarokat okozna** a nemzetgazdaságban, a közrendben vagy a társadalmi működésben. **Az elvárt kiberbiztonsági szint itt a legmagasabb, a felügyelet pedig intenzívebb.**

- Az érintett ágazatok: **energetika, közlekedés, egészségügy, vízszolgáltatók, szennyvíz szolgáltatás, hírközlési szolgáltatás, digitális infrastruktúra, kihelyezett IKT szolgáltatások, közigazgatás és űralapú szolgáltatások.**

- **Fontos szervezetek (Kockázatos ágazatok):** olyan szektorok és szervezetek tartoznak ebbe a kategóriába, amelyek bár fontosak, de a szolgáltatásaik megszakadása kevésbé súlyos vagy széleskörű hatással járna, mint az alapvető szervezetek esetében. **Kockázati szintjük jelentős, de a követelmények és az ellenőrzések enyhébbek lehetnek** az alapvető kategóriánál.

- Az érintett ágazatok: **postai és futárszolgálatok, élelmiszeripar (feldolgozás, gyártás és disztribúció), hulladékgazdálkodás, vegyszerek előállítása és forgalmazása, gyártás, digitális szolgáltatók, kutatás.**

Az ellátási láncok biztonsága kiemelten fontos a NIS2 irányelvben, mivel egyre inkább a kiberbiztonsági keretrendszerek fókuszába kerülnek. Mind az alapvető, mind a fontos **szervezeteknek biztosítaniuk kell, hogy beszállítóik és szolgáltatóik rendelkezzenek a megfelelő kiberbiztonsági intézkedésekkel** a kritikus szolgáltatások integritásának védelme érdekében. Ez magában foglalja az ellátási lánc kockázatainak hatékony kezelése érdekében bevezetett **auditok és kockázatértékelések elvégzését.**

Fontos megjegyezni, hogy **a NIS2 kötelezettségei közvetetten kiterjednek az ellátási láncban részt vevő beszállítókra és szolgáltatókra is.** Az érintett szervezetnek a beszállítóktól, szolgáltatótoktól meg kell követelniük, stabil alapokon nyugvó kiberbiztonsági intézkedéseket vezessenek be a kritikus szolgáltatásokhoz való hozzájárulásuk védelme érdekében.

Ennek eredményeként **az ellátási láncon belül minden félnek együtt kell működnie** a biztonság fokozása érdekében. Ezen túlmenően **az irányelv hatálya kiterjedhet azokra a nem uniós jogalanyokra is,** amelyek szolgáltatásokat vagy termékeket nyújtanak magyar, illetve uniós ügyfeleknek, különösen, ha jelentős jelenléttel vagy hatással rendelkeznek az EU piacán.

Kiberbiztonság mindenkinek? A NIS2 Irányelv átfogó érintettségi szempontjai Magyarországon

A NIS2 irányelv célja a kiberbiztonsági ellenállóképesség fokozása. Magyarországon a 2024. évi LXIX. törvény alapján ágazati és méretbeli kritériumok egyaránt érvényesülnek. Ez a megközelítés kiterjeszti a NIS2 irányelv hatálya alá tartozó szervezetek körét, ezzel biztosítva, hogy a kritikus ágazatokban működő, jelentős hatással bíró szervezetek – akár kisebb, de kiemelt fontosságú szereplők is – megfeleljenek a szigorúbb kiberbiztonsági követelményeknek.

A magyar jogszabály az "Alapvető szervezetek" számára szigorúbb előírásokat ír elő, mint a "Fontos szervezetek" számára. Az alkalmazandó intézkedések a kockázatarányos megfelelés érdekében mindig az értékelt kockázatoktól és a hazai jogszabályi környezettől függenek.

Fontos szűrő továbbá, hogy az ágazati besorolás mellett a vállalat mérete és árbevétele is meghatározó. E két kritérium közül elegendő az egyik teljesülése ahhoz, hogy a vállalat érintetté váljon.

Létszám szempontjából általánosságban elmondható, hogy az **50 fő feletti létszámú** szervezetek tartoznak a NIS2 irányelv hatálya alá, kivéve, ha ágazati jelentőségük miatt ettől függetlenül is kritikusnak minősülnek.

Árbevétel tekintetében pedig azok a szervezetek érintettek, amelyek **legalább évi 10 millió euró árbevétellel rendelkeznek,** amennyiben nem esnek az ágazati kritikus besorolás alá, amely automatikusan maga után vonja az érintettséget.

Önkormányzati érintettség

A 2024. évi LXIX. törvény új alapokra helyezte Magyarország kiberbiztonsági jogi környezetét, felváltva a korábbi szabályozást. Hatálya alá tartoznak mindazon önkormányzatok, amelyek közszolgáltatásokat nyújtanak vagy kritikus informatikai rendszereket üzemeltetnek.

Az érintett önkormányzatoknak kötelező kockázatkezelési intézkedéseket bevezetniük, incidenseket jelenteniük, és biztosítani a folyamatos megfelelést. A cél a közszolgáltatások zavartalan működésének és informatikai biztonságának garantálása.

A jogszabály a méret és a tevékenység jellege alapján különböző kategóriákba sorolja az önkormányzatokat, így nem minden érintett szervezetre vonatkoznak azonos szintű követelmények. Az arányos szabályozás érdekébe a kisebb önkormányzatokra egyszerűsített megfelelési eljárások és könnyebb adminisztratív szabályok vonatkoznak.

Minden érintett önkormányzatnak biztosítania kell az alapvető kockázatkezelési intézkedéseket, és készen kell állnia az incidensek bejelentésére, valamint a hatósági ellenőrzésekre. Így a szabályozás hozzájárul a közszolgáltatások biztonságához, miközben figyelembe veszi az önkormányzatok kapacitásait és adottságait.

Ha kérdése van, vagy bizonytalan abban, hogy milyen feladatokkal jár a jogszabályi megfelelés az önkormányzat számára, forduljon bizalommal szakértő kollégáinkhoz a **ctrl_solutions@telekom.hu** címen. Szívesen segítünk a felkészülésben és a jogszabályoknak való megfelelésben!

A NIS2 szankciórendszer: Miért és Hogyan?

A NIS2 irányelv bevezetésének célja, hogy valódi jogi kötelezettségeket teremtsen a kiberbiztonság terén, és **szankciók, büntetések** bevezetésével garantálja azok betartását. A súlyos következmények elrettentő erővel bírnak, biztosítva a kritikus szolgáltatások folytonosságát és a kiberbiztonsági szabályok uniós szintű harmonizációját, növelve az elszámoltathatóságot és a bizalmat a digitális tér iránt.

A hatósági szankciók a hazai jogszabály alapján többlépcsősök lehetnek, a jogsértés súlyától függően:

· **Figyelmeztetés és felszólítás a hiányosságok pótlására:** Első lépésként a hatóság (pl. SZTFH) határidőt szabhat a hiányosságok orvoslására.

· **Tevékenységtől való eltiltás:** Súlyosabb vagy ismétlődő jogsértés esetén az SZTFH döntése alapján az adott szolgáltatás vagy tevékenység végzésétől való eltiltásra is sor kerülhet.

· **Szolgáltatásban résztvevők tájékoztatása:** Előírható, hogy az érintett szervezet tájékoztassa a szolgáltatásban résztvevőket a fenyegetésekről.

· **Ismételten kiszabható bírság:** A szabályozás lehetővé teszi ismételhető bírságok kiszabását. Ezek jelentős összegűek lehetnek, és a jogsértések súlyától, valamint a szervezet típusától és méretétől függően változhatnak.

A szankciók jellege és mértéke mindig arányos a szabálysértés súlyával, az okozott kárral, és a szervezet nagyságával.

A szervezeti szankciók

A NIS2 irányelvet átültető hazai jogszabály be nem tartása jelentős pénzügyi és működési szankciókat vonhat maga után, melyek mértéke a szervezet típusától és a jogsértés súlyosságától függően változik a **2024. évi LXIX. törvényben és a hozzá kapcsolódó 418/2024. (XII. 23.) Kormányrendeletben foglaltak szerint:**

Pénzbírságok

- **Alapvető szervezetek (Kiemelten kockázatos ágazatok)**
  A maximális bírság elérheti a 10 millió eurót, vagy az éves összforgalom 2%-át.
- **Fontos szervezetek (Kockázatos ágazatok)**
  A bírság plafonja 7 millió euró, vagy a vállalat előző évi forgalmának 1,4%-a.

Minden esetben a magasabb összeg alkalmazandó.

Az egyedi szankciók

Változás az elszámoltathatóságban

A NIS2 és annak alapján a hazai szabályozás újradefiniálja a szervezeten belüli kiberbiztonsági felelősséget, amely így az informatikai részleg felelősségi köréből a vezetői csapatába kerül, így a felsővezetők napirendjének fontos pontjává válik. Ez a változás a felsővezetők kötelességét emeli ki, ezzel biztosítva a hatékony kockázatkezelést és a kiberbiztonsági felügyeletet.

A NIS2 irányelv szerinti szervezeti szankciók mellett **a magyar szabályozás alapján a felsővezetők személyesen is felelősségre vonhatók** a kiberbiztonsági jogszabályi előírásokban foglaltak be nem tartásáért, különösen súlyos gondatlanság esetén. Ez magában foglalhatja a nyilvánosságra hozatalt vagy akár a **tevékenységtől való eltiltást.** A magyar kormányrendelet értelmében a bírság összege elérheti a 150 millió forintot, és a jogsértés súlyosságától függően **büntetőjogi szankciók is alkalmazhatók** lehetnek.

A felsővezetői kör felelőssége a NIS2 szerint

Felelős szerepkör vagy gazdasági szerep *	**A NIS2 végrehajtásához szükséges intézkedések**
CEO-VEZÉRIGAZGATÓ	A végrehajtás felügyelete és felelősségvállalás
CSO, jogi terület	Kockázatelemzés és a vállalat információs rendszerbiztonsági politikája (ISSP)
CSO, CIO / CTO	Incidensek kezelése
CIO / CTO, CSO	Üzletmenet-folytonosság, például biztonsági mentés, katasztrófa utáni helyreállítás és válságkezelés
CSO, beszerzés, jogi terület	Ellátási lánc biztonsága, beleértve a beszállítókkal vagy szolgáltatókkal való kapcsolatok biztonsági szempontjait is
CSO, CIO/CTO, beszerzés, jogi terület	Biztonság a hálózatok és információs rendszerek beszerzése, fejlesztése és karbantartása során, beleértve a sebezhetőség kezelését is
CSO	A kiberbiztonsági kockázatkezelési eljárások és politikák hatékonyságának értékelése
CSO, HR	Alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzés
CSO, CIO / CTO	A kriptográfiára és adott esetben a titkosításra vonatkozó irányelvek és eljárások.
CSO, CIO / CTO, HR	Személyzeti biztonság, személyazonosság-kezelés és hozzáférés-ellenőrzés, valamint eszközkezelési politikák
CSO, CIO / CTO	Többfaktoros vagy folyamatos autentikáció, biztonságos kommunikáció (hang, szöveg, videó) és vészhelyzeti protokollok használata.

Az e feladatokért való felelősség változhat
a szervezet méretétől és felépítésétől függően. Kisebb vállalkozásoknál például az üzlet tulajdonosa több szerepet is betölthet.

NIS2-es szakértőink támogatást nyújtanak abban is, hogy a követelményeknek leginkább megfelelő csapatot állítsák össze, és pótolják az esetleges hiányosságokat is!

NIS2 Készültség: Felmérés és Szabályozás

Ha felmérné szervezetének jelenlegi NIS2-es megfelelőségi szintjét, javasoljuk, hogy vegye igénybe a Telekom Gap analízis szolgáltatását.

Ez az analízis egy alapos kiberbiztonsági értékelés, amely segít Önnek felmérni, hogy szervezete mennyire felel meg a 2024. évi LXIX. törvénynek (Kibertan. tv.) és a vonatkozó rendeleteknek. **A Telekom szakemberei segítséget nyújtanak a hiányosságok feltérképezésében és ajánlásokat fogalmaznak meg a megfelelő intézkedések bevezetésére, ami az első lépések egyike az auditra való felkészülésben.**

- **Alapvető és fontos szervezetek (Kiemelten kockázatos és kockázatos ágazatok):** Ezek a **2024. évi LXIX. törvény (Kibertan. tv.) által alapvető vagy fontos szervezeteknek minősített szervezetek.** A kijelölt nemzeti hatóság, a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH), **felügyeli és ellenőrzi ezen szervezetek jogszabályi kötelezettségeinek betartását.** Emellett aktívan reagál a bejelentett kiberbiztonsági eseményekre és incidensekre, szükség esetén vizsgálatokat indítva és intézkedéseket téve.

A **Telekom tapasztalt szakértői csapata kész segítséget nyújtani** Önnek abban, hogy felkészüljön a 2024. évi LXIX. törvény (Kibertan. tv.) által támasztott kihívásokra, és biztosítsa vállalkozása kiberbiztonsági ellenállóképességét.

Forduljon hozzánk bizalommal, hogy mihamarabb megkezdhessük a felmérést és a szükséges fejlesztések tervezését!

Incidensjelentés a NIS2 szabályozás alapján

Három fázisú protokoll

Fedezze fel a Telekom NIS2 szolgáltatásait.

A magyar 2024. évi LXIX. törvény (Kibertan. tv.) **szigorú és strukturált jelentési rendszert** vezet be a jelentős kiberbiztonsági incidensek kezelésére, **amelyek súlyosan érinthetik** egy szervezet működését, hálózati és információs rendszereinek biztonságát, vagy az általa biztosított szolgáltatások folytonosságát. A jelentős kiberbiztonsági incidensek bejelentése egy háromlépcsős folyamat, amely a következőkből áll:

1

Korai figyelmeztetés: A súlyos hatású, jelentős incidenst **haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül be kell jelenteni az SZTFH-nak.** Ennek célja a gyors beavatkozás és a hatások megfékezése. Az első értesítésnek tartalmaznia kell az incidens jellegére és súlyosságára vonatkozó alapinformációkat.

2

Értesítés az incidensről: Az első bejelentést követően, **legkésőbb 72 órán belül részletesebb előzetes jelentést kell benyújtani** az SZTFH-nak. Ennek tartalmaznia kell az incidens első értékelését: súlyosságát, lehetséges következményeit, okait és a kezdeti intézkedéseket, segítve ezzel a hatóságot a pontosabb helyzetfelmérésben és a koordinációban.

3

Zárójelentés: Az incidens kezelése és lezárása után, legkésőbb egy hónapon belül (az előzetes jelentéstől vagy a lezárástól számítva) **egy átfogó zárójelentést kell küldeni** az SZTFH-nak. Ez bemutatja az incidens lefolyását, a megtett intézkedéseket, hatásokat, gyökérokokat, tanulságokat és a jövőbeni megelőző lépéseket.

A magyar 2024. évi LXIX. törvény (Kibertan. tv.) felhatalmazza a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH) az incidensbejelentési szabályok meghatározására és betartatására. Az SZTFH látja el a nemzeti CSIRT (Computer Security Incident Response Team) feladatait, felügyelve a bejelentéseket és a reagálást.

Hogyan kell felkészülni a NIS2 megfelelésre?

Helyezze a hangsúlyt három fő területre – a technikai, eljárási és üzemeltetési vagy operatív oldalra –, és kezelje a kiberbiztonsági kockázatokat átfogó módon: megelőzéssel, felismeréssel, gyors reagálással és hatékony elhárítással.

Ismerje meg a Telekom NIS2 megoldásait

Technikai

- **Erős és biztonságos rendszerek fejlesztése, amelyek megvédenek a kiberfenyegetésekkel szemben:** A Telekom CTRL 360 Menedzselt Határvédelem és Végpontvédelem szolgáltatásaival erősíthető a rendszerek kiberfenyegetésekkel szembeni ellenállóképessége.
- **Korai figyelmeztető rendszerek és eseménykezelési mechanizmusok létrehozása:** A Telekom IBFaaS szolgáltatása és a CTRL SIEMaaS/ CTRL SOC szolgáltatásai biztosítják a valós idejű monitorozást, a támadásokra való gyors reagálást és a jogszabályi előírásoknak való informatikai megfelelést.
- **Átfogó katasztrófa utáni helyreállítási tervek végrehajtása:** A Telekom BaaS (Backup as a Service) bevezetése kritikus fontosságú lehet az adatok és rendszerek gyors helyreállításához egy incidens után.
- **Hatékony hozzáférés-ellenőrzési és hitelesítési intézkedések:** A Telekom OKTaaS, mint e-learning platform segíti a felhasználók biztonságtudatosságának növelését és felkészültségét, míg a Telekom MobileSecurity szolgáltatás megvédi mobileszközeinket az illetéktelen hozzáféréstől.

Eljárásrendi

- **A rendszeres infrastrukturális biztonsági értékelések** elengedhetetlenek a sebezhetőségek azonosításához. A Telekom CTRL Sérülékenység Menedzsment és CTRL Penetrációs teszt szolgáltatása, valamint a CTRL Menedzselt Végpont és CTRL Menedzselt E-mail Védelem szolgáltatások biztosítani tudják a folyamatos monitorozást és védelmet.
- **A kiberbiztonsági ellenőrzések hatékonyságának mérése** alapvető feladat a jogszabályi megfeleléshez és a folyamatos fejlődéshez. A Telekom GAP analízis, IBFaaS / IBF Mentor szolgáltatások támogatni tudják ennek a célnak az elérését.
- **A kiberbiztonsági tudatosság előmozdítása és a HR biztonsági protokollok javítása** csökkenti a belső kockázatokat. A Telekom OKTaaS bevezetése kifejezetten a képzéseket célozza, míg az IBFaaS / IBF Mentor, valamint az IBSZ elkészítése segíti a HR biztonsági eljárásokat.
- **Az alkalmazottak bevonása a biztonsági kultúrába** elengedhetetlen a közös felelősségérzet kialakításához. Az OKTaaS szolgáltatás révén a Telekom növelni tudja a tudatosságot és erősíti a biztonsági kultúrát.

Operatív

- **Átfogó szabályzat- és eljárásrend létrehozása:** A Telekom Gap analízis szolgáltatásával felméri a meglévő állapotot, majd az IBSZ elkészítése (Információ Biztonsági Szabályzat) szolgáltatással segíti a jogszabályok szerinti szabályzatok és eljárások kidolgozását.
- **Rendszeres felülvizsgálat és frissítés:** A Telekom Gap analízis szolgáltatás és az IBFaaS / IBF Mentor szolgáltatások segítik a szervezetet a folyamatos felülvizsgálatban, a változásokhoz való alkalmazkodásban és a jogszabály informatikai megfelelés fenntartásában.
- **Incidensbejelentési kötelezettségek:** A Telekom IBFaaS szolgáltatás kifejezetten az incidensbejelentési kötelezettségek teljesítését támogatja, beleértve a határidők betartását és a megfelelő formátumot.
- **Kockázatkezelési folyamat:** A CTRL Sérülékenység Menedzsment és CTRL Penetrációs Teszt szolgáltatások, valamint a Gap analízis szolgáltatás is használható harmadik fél értékelésekhez, hozzájárulva az ellátási lánc kockázatainak felméréséhez és kezeléséhez.

Hogyan segíthetünk?

Fedezze fel az alábbi jogszabályi informatikai megfelelést támogató szolgáltatásainkat vagy vegye fel velünk a kapcsolatot, és kérjen díjmentes konzultációt!

Mindent egy helyen

- GAP analízis
- IBFaaS
- OKTaaS
- CTRL 360 Menedzselt E-mail védelem
- Telekom MobileSecurity
- CTRL SWAT basic
- CTRL 360 Menedzselt Határvédelem
- CTRL 360 Menedzselt Végpontvédelem

Miért a Magyar Telekom?

Hírközlési szolgáltatóként szigorú előírások szerint működünk, és megfelelünk a jogszabályi előírásoknak. Tisztában vagyunk az Ön előtt álló kihívásokkal, és segítünk csökkenteni a megfelelésből adódó terheket – így biztos lehet benne, hogy szervezete felkészült lesz a NIS2 irányelv elvárásaira, és hatékonyan fog tudni védekezni a kibertámadásokkal szemben.
Széles körű IT-biztonsági szolgáltatásaink mellett olyan, kifejezetten a NIS2 előírásaira szabott megfelelőségi csomagokat is kínálunk, amelyek célzottan támogatják Önt a hazai jogszabályi követelmények teljesítésében.

Vegye fel velünk a kapcsolatot a **ctrl_solutions@telekom.hu** email címen, és segítünk megtalálni a legjobb megoldást!

Connecting your world.

Magyar Telekom Nyrt.