# NIS2 és kiberbiztonság – Mi a teendője egy KKV-nak?

A NIS2 (Network and Information Systems Directive 2 az Európai Parlament és a Tanács (EU) 2022/2555 irányelve a magas szintű kiberbiztonság biztosításáról) 2024 óta rengeteg magyarországi cég kiberbiztonsági előírásait és technológiai megoldásait reformálta meg, amelyet a hazai jogrendbe a Magyarország kiberbiztonságról szóló 2024. évi LXIX. törvény ültetett át. Korábban már írtam az EU-s irányelvről, jelen cikkemben egy kis történeti áttekintést és a jövőben várható feladatokról is lesz szó, hiszen a 2026-tól azon KKV-k is érintettek lehetnek, amelyek beszállítói egy NIS2 kötelezett cégnek.

## A közelmúlt: Hogyan jutottunk el a felkészüléstől a könnyítésekig?

A hazai kiberbiztonság új időszámítása a 2024. évi LXIX. törvény hatálybalépésével kezdődött. Ez a szabályozás a meghatározott kockázatos és kiemelten kockázatos ágazatokban működő azon vállalatokat kötelezte digitális védelmi vonalaik felülvizsgálatára, amelyek a törvényi kritériumok szerint legalább középvállalkozásnak minősültek. Az első kritikus határidő a kötelező regisztráció volt a felügyeletet ellátó Szabályozott Tevékenységek Felügyeleti Hatóságánál (SZTFH), amelyet az addig már működő érintett cégeknek 2024. június 30-ig kellett teljesíteniük.

A vállalkozásoknak emellett törvényi kötelezettségük volt egy önálló Informatikai Biztonsági Felelős (IBF) kijelölése. Az IBF feladata lett a kockázatelemzés elkészítése és a kötelező kiberbiztonsági osztályba sorolás végrehajtása, valamint a folyamatos fenntarthatóság biztosítása.

A gyakorlati megvalósítás során azonban a hazai vállalkozások komoly erőforrás- és szakemberhiánnyal szembesültek. Felismerve a KKV és középvállalati szektor leterheltségét, a kormányzat a Magyar Kereskedelmi és Iparkamarával (MKIK) egyeztetve jelentősen módosította az eredeti menetrendet, és könnyítéseket vezetett be a kötelezettségek ütemezésében:

A szerződéskötési könnyítés: Bár az első hivatalos kiberbiztonsági auditot korábban tervezték lezárni, a cégek haladékot kaptak. Cserébe a hatóság előírta, hogy 2025. augusztus 31-ig minden érintett vállalatnak kötelezően le kellett szerződnie egy hivatalos, az SZTFH által nyilvántartásba vett kiberbiztonsági auditor céggel.

Költségvédelmi kedvezmények: A cégek anyagi védelme érdekében a jogalkotó külön rendeletekben maximalizálta a felmerülő költségeket. Különválasztották az SZTFH felé fizetendő, sávos rendszerű éves kiberbiztonsági felügyeleti díjat – amelynél egy méltányos felső plafont szabtak meg –, valamint a kötelező kiberbiztonsági audit díját. Utóbbit hatósági árassá tették, így a független auditorok nem kérhetnek a rendeletben rögzített maximum kalkulált alapdíjaknál és szorzóknál magasabb összeget a vizsgálatért, védve ezzel a vállalkozásokat a piaci áremelkedésektől.

Az audit-haladék: A piac tehermentesítése érdekében a jogalkotó fél év haladékot biztosított az átvilágítások tényleges befejezésére. Így az első kötelező hatósági kiberbiztonsági audit lefolytatásának végső határideje 2026. június 30. lett.

**Feladatok a kiberbiztonsági audit lezárása után:**

Az audit határidejének lejárta nem a folyamat végét, hanem egy új, folyamatos védelmi ciklus kezdetét jelenti a vállalatok számára. Az átvilágítás lezárását követően az érintett cégeknek az alábbi kötelező lépésekkel kell tovább haladniuk:

Az auditjelentés benyújtása: Az auditot végző szervezet a vizsgálat végén egy részletes auditjelentést és tanúsítványt állít ki. Ezt a dokumentumot a jogszabályban meghatározott rövid határidőn belül elektronikusan fel kell tölteni az SZTFH hivatalos ügyintézési felületére.

Hiányosságok kötelező javítása: Ritka, hogy egy rendszer elsőre hibátlan legyen. Ha az auditor hiányosságokat vagy kockázatokat tár fel, a vállalkozásnak egy kötelező intézkedési tervet (javítási ütemtervet) kell kidolgoznia.

A javító intézkedések végrehajtása: A jogszabály által biztosított határidőn belül a cég köteles végrehajtani a tervben vállalt informatikai és védelmi fejlesztéseket. Ez a türelmi idő lehetőséget ad a hibák javítására anélkül, hogy a hatóság azonnal szankcionálna.

Rendszeres felülvizsgálat: A kiberbiztonság nem egyszeri projekt. A cégeknek gondoskodniuk kell arról, hogy az Informatikai Biztonsági Felelős (IBF) folyamatosan nyomon kövesse a fenyegetéseket, és az auditált védelmi szintet a mindennapokban is fenntartsa.

Kétéves auditciklus: A törvény értelmében a kiberbiztonsági auditot kétévente kötelező megismételni. Ez biztosítja, hogy a digitális védelmi vonalak a technológia fejlődésével és az új típusú kibertámadásokkal együtt változzanak.

**A jövő: Mi lesz a piac többi szereplőjével?**

A NIS2 szabályozás két teljesen különböző módon alakítja át a KKV-szektor mindennapjait: míg a jogalkotó igyekszik megvédeni a kisebb cégeket a közvetlen adminisztrációs terhektől, a piaci realitás miatt szinte egyetlen vállalkozás sem vonhatja ki magát a hatások alól.

A közvetlen érintettség terén a főszabály szerint a mikro- és kisvállalkozások a jövőben is általános mentességet élveznek, így nem kell regisztrálniuk az SZTFH-nál és mentesülnek a kötelező hatósági kiberbiztonsági audit alól is. Ez alól kizárólag azok a speciális, mérettől független digitális területeken működő KKV-k jelentenek kivételt, mint például a közcélú hírközlési szolgáltatók, a DNS-szolgáltatást nyújtók, a legfelső szintű domainnév-nyilvántartók vagy a bizalmi szolgáltatók, amelyeknél a tevékenység jellege miatt elengedhetetlen a szigorú felügyelet.

A szektor döntő többségét azonban a közvetett érintettség, vagyis az úgynevezett ellátási lánc hatás fogja utolérni a közeljövőben. A NIS2 törvény ugyanis kötelezi a hatálya alá tartozó vállalatokat, hogy vizsgálják felül a teljes beszállítói láncuk kiberbiztonsági kockázatait. Ez azt jelenti, hogy ha egy KKV beszállítóként, IT-üzemeltetőként, szoftverfejlesztőként, vagy akár alvállalkozóként kapcsolódik egy ilyen kötelezett szervezethez, a jövőben csak akkor tarthatja meg a megbízásait, ha írásban és igazolható módon garantálni tudja a saját digitális védelmi szintjét vagy az őt megbízó szervezet egyértelműen elfogadja az ebből adódó maradvány-kockázatokat.

A nagyvállalatok a saját megfelelésük érdekében kénytelenek lesznek kiszelektálni azokat a partnereket, amelyek biztonsági rést jelentenek a rendszereikben, így a kiberbiztonság a KKV-k számára a jövőben már nem egy felesleges informatikai kiadás, hanem a piacon maradás és a versenyképesség alapfeltétele lesz.

Erre a piaci nyomásra a KKV-szektor leginkább az önkéntes megfelelés útjára lépve tud hatékony választ adni a jövőben. Ez azt jelenti, hogy a kisebb vállalkozások – bár jogilag nem kötelezi őket az SZTFH regisztráció – saját jól felfogott üzleti érdekükből, proaktívan elkezdik átvenni és bevezetni a NIS2 keretrendszer alapvető védelmi intézkedéseit. Ez a gyakorlatban nem jelent megfizethetetlen beruházásokat, sokkal inkább olyan alapvető biztonsági rutinok kialakítását foglalja magában, mint a kétlépcsős azonosítás kötelezővé tétele, a titkosított és elszeparált biztonsági mentések rendszere, az informatikai rendszerek rendszeres frissítése, valamint a munkavállalók folyamatos kiberbiztonsági tudatossági képzése. Az önkéntes megfelelés legnagyobb előnye, hogy a KKV-k hivatalos és költséges audit nélkül is felkészültté válnak a megrendelői auditokra és átvilágítási kérdőívekre. Ezzel a lépéssel a cégek nemcsak a meglévő partnerségeiket betonozzák meg, hanem komoly piaci előnyre is szert tesznek, hiszen a biztonságtudatos működés felmutatásával könnyebben nyerhetnek el új, értékes nagyvállalati vagy akár állami megrendeléseket is a kevésbé felkészült versenytársaikkal szemben.

Hajdara Gábor