Hidrogéntechnológiákhoz kapcsolódó főbb kiberbiztonsági elvárások

NIS2, hazai szabályozás és EU-s projektkövetelmények

Napjainkra a kiberbiztonság az energetika, illetve a fontosabb technológiák esetében is megkerülhetetlen követelménnyé vált. Így van ez a hidrogéntechnológiák terén is, amelyet a kiberbiztonsági irányelv, illetve a hazai kiberbiztonsági (2024. évi LXIX.) törvény 2. melléklete kifejezetten nevesíti a „***kiemelten kockázatos ágazatokban*** *működő szolgáltatók és szervezetek*” között:

- ágazat: Energetika / alágazat: Hidrogén
- szervezet típusa: **a hidrogéntermelés, -tárolás és -szállítás üzemeltetője**

Jogszabályi háttér

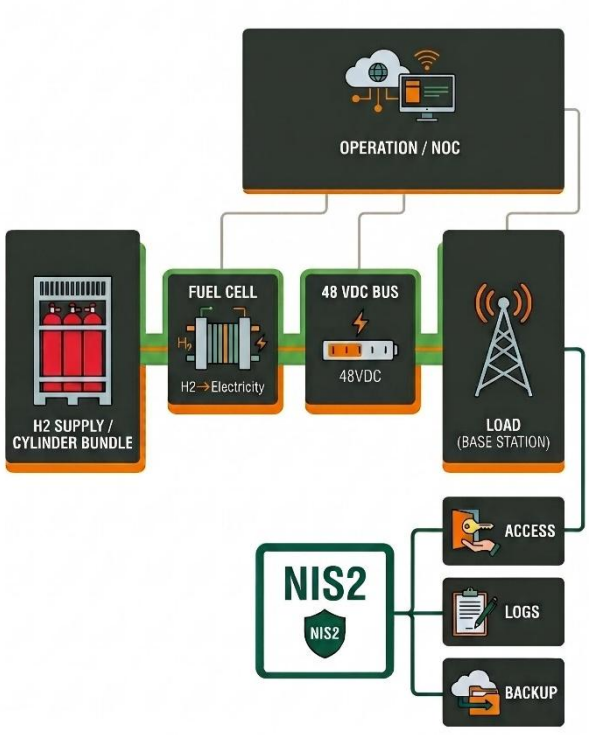
(EU) 2022/2555 irányelv (NIS2 irányelv) *az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről*

2024. évi LXIX. törvény *Magyarország kiberbiztonságáról (amely a NIS2 irányelven alapuló nemzeti jogszabály), valamint az ennek végrehajtását leíró SZTFH rendeletek*

Mit jelent a „kiemelten kockázatos ágazat” a hidrogéntechnológiák esetében információbiztonsági szempontból? A „*kiemelten kockázatos ágazat*” minősítés a hidrogéntermelés, -tárolás és -szállítás üzemeltetői esetében nem egyszerűen azt jelenti, hogy az adott szervezetnek megfelelő irodai informatikával kell rendelkeznie. A NIS2 és a hazai kiberbiztonsági szabályozás logikája ennél szélesebb: a cél az érintett szolgáltatások működésének, ellenállóképességének és biztonságának megerősítése.

Hidrogéntechnológiai környezetben ezért nemcsak a klasszikus IT-rendszerekre kell gondolni, mint a levelezés, dokumentumkezelés, vállalatirányítás, felhasználói jogosultságkezelés vagy mentés. Legalább ilyen fontosak lehetnek az ipari OT-rendszerek is: szenzorok, PLC-k, HMI/SCADA felületek, mérnöki munkaállomások, távoli karbantartási hozzáférések, adatgyűjtők, naplózási rendszerek, valamint a beszállítói és üzemeltetői kapcsolatok.

A hidrogéntechnológiai üzemeltetőnek ebből következően kockázatalapú szemléletben kell vizsgálnia a rendszereit. Meg kell tudni határozni, mely elektronikus információs rendszerek kapcsolódnak a kritikus működéshez, kik férnek hozzá ezekhez, milyen módon történik a távoli üzemeltetés vagy karbantartás, hogyan észlelhető egy incidens, és milyen lépések biztosítják a biztonságos működés helyreállítását.



A hazai szabályozás az érintett szervezetek számára többféle szervezeti és technikai kötelezettséget is jelenthet. Ide tartozhat az érintettség megállapítása, a szükséges bejelentési vagy nyilvántartásba vételi kötelezettségek teljesítése, az elektronikus információs rendszerek azonosítása és biztonsági osztályba sorolása, a kockázatok felmérése, a megfelelő védelmi

intézkedések kialakítása, az incidenskezelési képesség megteremtése, a beszállítói kockázatok kezelése, valamint az auditálhatóság biztosítása. A vezetői felelősség szintén lényeges elem: a kiberbiztonság ilyen környezetben nem kizárólag az informatikai szervezet belügye.

Fontos pontosítás, hogy a NIS2 és a magyar kiberbiztonsági törvény nem úgy működik, hogy minden hidrogéntechnológiai szereplő számára egyetlen konkrét kiberbiztonsági szabványt tesz kötelezővé. Nem mondható például, hogy az ISO/IEC 27001 tanúsítás önmagában automatikus NIS2-megfelelést jelentene. A szabályozás inkább követelményrendszert, felelősségi keretet, hatósági láthatóságot, auditálhatóságot és kockázatalapú védelmi gondolkodást vár el.

A szabványok ugyanakkor fontos gyakorlati kapaszkodót adhatnak. Az ISO/IEC 27001 az információbiztonsági irányítási rendszer, az IEC 62443 az ipari automatizálási és vezérlőrendszerek kiberbiztonsága, az ISO 22301 pedig az üzletmenet- és működésfolytonosság területén nyújthat jól használható keretet. Ezek nem egymást helyettesítő, hanem egymást kiegészítő megközelítések: más réteget fed le a szervezeti irányítás, az OT-biztonság, a működésfolytonosság és a technológiai megfelelés.

Gyakori kérdés, hogy a hidrogéntermelés, -tárolás vagy -szállítás esetében vannak-e mennyiségi küszöbértékek, például t/nap, kg/óra, MW vagy tárolókapacitás alapján. A kiberbiztonsági törvény hidrogénre vonatkozó mellékleti sora nem tartalmaz ilyen kapacitásküszöböt, hanem a tevékenységhez és az üzemeltetői szerephez kötött szervezeti kategóriát használ: a hidrogéntermelés, -tárolás és -szállítás üzemeltetőjét nevesíti. A gyakorlati érintettség megállapításához ezért nem elegendő pusztán műszaki kapacitásadatokat nézni, vizsgálni kell, hogy az adott szervezet milyen jogi, üzemeltetői és szolgáltatási szerepben vesz részt a hidrogénhez kapcsolódó tevékenységben.

Különösen indokolt az egyedi vizsgálat pilot, K+F, demonstrációs, laboratóriumi, beszállítói vagy rendszerintegrátori szerepkörök esetén. Egy kis kapacitású vagy kutatási célú rendszer nem feltétlenül azonos megítélés alá esik egy ipari termelő-, tároló- vagy szállítóüzemmel, ugyanakkor szerződéses, beszállítói, pályázati vagy üzemeltetési követelmények alapján ezeknél is megjelenhetnek kiberbiztonsági elvárások.

Összességében tehát a hidrogénágazati NIS2-érintettség információbiztonsági szempontból nem szűkíthető le a hagyományos vállalati IT védelmére. Az érintett szervezetnek a teljes digitális működési környezetet vizsgálnia kell: az irodai IT-t, az OT/SCADA rendszereket, a távoli hozzáféréseket, a beszállítói kapcsolatokat, a naplózást, az incidenskezelést és a működésfolytonosságot is. A megfelelés célja nem pusztán az adminisztratív kötelezettségek teljesítése, hanem a biztonságos, átlátható, auditálható és zavar esetén is helyreállítható működés.

A hidrogéntermelésen belül az elektrolizálók a jövőben jelentős energiafogyasztóként és hálózatba integrált ipari rendszerekként működhetnek. Ipari vezérlésük, távfelügyeletük és adatkapcsolataik miatt OT/SCADA környezetük kritikus jelentőségű lehet. A hidrogéntechnológiák sajátossága, hogy a fizikai folyamatok, az automatizált vezérlés, a távoli menedzsment, valamint az IT-, OT- és safety-rendszerek szorosan összekapcsolódnak. Ezért egy kiberbiztonsági incidens nemcsak adatvesztést vagy informatikai szolgáltatáskiesést okozhat, hanem érintheti a technológiai folyamatot, a riasztásokat, a védelmi funkciókat és szélsőséges esetben a személy- vagy vagyonbiztonságot is. A NIS2 hidrogénipari értelmezése így közelebb kerül az ipari működésbiztonsághoz, mint a klasszikus irodai IT-biztonsághoz.

Közvetett érintettség: a hidrogéntechnológiák nemcsak a 2. mellékletben nevesített hidrogéntermelés, -tárolás és -szállítás révén kapcsolódhatnak a NIS2-höz és a hazai kiberbiztonsági szabályozáshoz. Közvetett érintettség is felmerülhet olyan ágazatokban, amelyek önállóan is kiemelten kockázatos vagy kockázatos ágazatnak minősülnek, és működésük során hidrogénalapú technológiát alkalmaznak. Ilyen lehet például a közösségi közlekedés, a vasúti közlekedés, az energetikai integráció vagy egyes ipari felhasználások. Ilyenkor a kiberbiztonsági követelmények nem feltétlenül a hidrogén önálló ágazati besorolásából, hanem az adott szolgáltatás, infrastruktúra vagy üzemeltetési környezet kockázataiból következnek.

Egyéb pályázati és szerződéses kiberbiztonsági elvárások: a NIS2 irányelven, illetve nemzeti jogon kívül más EU-s eszközök is elvárhatják a hidrogénprojektek kiberbiztonságát. Az egyik fontos ilyen példa az Európai

Hidrogén Bank (EHB) éves rendszerességű aukciós kiírásai, pontosabban azok általános szerződési feltételei (*Terms & Conditions*). Az EHB pályázat szerződéses feltételei nem említik explicit módon a NIS2 irányelvet, de szakmai és projektkockázati szempontból egy modern hidrogénprojektnek célszerű a NIS2 szemléletével összhangban álló kiberbiztonsági érettséget kialakítania. Ez várhatóan a bankképesség (*bankability*) megítélése szempontjából is egy kifejezetten elvárt faktor lesz. Az EHB nem egy részletes, konkrét technikai kontroll-lista, hanem inkább magas szintű megfelelési elvárás. Ami kötelező, hogy a projekteknek biztosítaniuk kell a biztonságos H_2-előállítási folyamatot és a megfelelő kibervédelmet (konkrétan idézve: *„appropriate safety and cyber-security requirements"; „compliance with … safety and cybersecurity standards"*) Ez tehát jogilag kötelező megfelelési kategória, de nem konkrét technikai specifikáció. Egyes pályázati vagy szerződéses feltételek az adatkezelés, az operatív kontroll és az adattárolás földrajzi helyére is tartalmazhatnak előírásokat, például az Európai Gazdasági Térség (EGT) belüli kezelésre vonatkozóan.

Milyen előírások, szabványok mentén célszerű, érdemes felépíteni egy hidrogénprojekt kiberbiztonságát:

- NIS2 alignment - jogszabályi megfelelés, kockázatkezelés, incidenskezelés, vezetői felelősség
- IEC 62443 - ipari automatizálási és vezérlőrendszerek, OT/SCADA security
- ISO/IEC 27001 - információbiztonsági irányítási rendszer, szervezeti kontrollok, governance
- ISO 22301 - business continuity, üzletmenet- és működésfolytonosság

Készítette:
Lóth Tamás, Teletom Kft. (www.teletom.hu)
Mayer Zoltán, MHT Egyesület (www.hfc-hungary.org)

Forrás:

European Commission: NIS2 Directive: securing network and information systems.