A magyar energiaszektor kiberbiztonsági fenyegetettségei

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

A magyar energiaszektor kiberbiztonsági fenyegetettségei

Vezetői összefoglaló

A magyar energiaszektor kiberbiztonsági fenyegetettsége az elmúlt években **nem egyszerűen nőtt, hanem jellegében változott meg**. A fenyegetettségi kép ma két, egymást erősítő folyamat metszetében alakul: **a szektor digitális átalakulása** – a termelés decentralizációja és az ipari vezérlőrendszerek hálózati integrációja – folyamatosan bővíti a támadható felületet, miközben a geopolitikai környezet a korábbinál kiszámíthatatlanabbá tette az energetikai infrastruktúra elleni műveletek valószínűségét. E tanulmány ezt a fenyegetettségi képet elemzi a Cyber Threat Intelligence (a továbbiakban: CTI) szemléletében, a magyar szektor szerkezeti sajátosságaira építve, a nemzetközi incidenseket elemzési referenciaként kezelve.

Az elemzés központi megállapítása, hogy a magyar szektor kockázati profilját **nem a legfejlettebb fenyegetés, hanem a legkevésbé védett réteg határozza meg**. A szektor **érettségi szintek szerint erősen rétegzett**: a néhány nagy, rendszerszinten kritikus üzemeltető védelmi kapacitása lényegesen magasabb, mint a távhőszolgáltatói, a kisebb beszállítói vagy a gyorsan bővülő decentralizált termelői rétegé. A fenyegető szereplők – az opportunista kiberbűnözéstől a peremréteget célzó hacktivizmuson át az államilag támogatott műveletekig – következetesen **a legkisebb ellenállás irányát keresik**, így a rendszerszintű kockázat éppen a leggyengébben felügyelt pontokon koncentrálódik.

A fenyegetés természete emellett **a láthatóból a látens felé tolódik**. A legfejlettebb szereplők jellemzően nem azonnali károkozásra, hanem a hálózatokba való csendes behatolásra és a hozzáférés fenntartására törekszenek, amelyet egy későbbi, politikai döntéstől függő időpontban aktiválhatnak. Ennek két következménye van a döntéshozók számára: **a látható incidensmentesség nem azonosítható a rendszerek érintetlenségével**, a fenyegetettségi szint pedig új behatolás nélkül is megugorhat, pusztán a geopolitikai helyzet romlásával. A védelmi képességet ezért nem a nyugalmi időszak, hanem **a feltételezhető csúcsterhelés szintjéhez kell méretezni**.

A tanulmány következtetései öt döntéshozói prioritásba rendeződnek. A legnagyobb határhaszon **a védelmi képesség rétegek közötti kiegyenlítésében** keletkezik, elsősorban a szűkös szaktudás megosztott, központi szolgáltatásként való elérhetővé tételével. A védelem súlypontját a

megelőzésről **a folyamatos észlelés és a rejtett hozzáférések aktív felderítése felé** kell tolni. A **beszállítói** és **karbantartói bizalmi hozzáféréseket** tényleges **felügyelet** alá kell vonni, mivel ezek **megkerülik** a hagyományos **peremvédelmet**. A **decentralizált termelés vezérlési rétegét** – amely fizikailag szétaprózott, de néhány gyártói platformon logikailag újrakoncentrálódik – **rendszerszintű kockázatként** kell kezelni. Végül a védelmi képesség felső határát meghatározó **szakemberhiány oldása** a többi prioritás előfeltétele, amelynek reális útja a meglévő szaktudás megosztásának intézményesítése. Ezek a **prioritások** együtt nem a fenyegetés megszüntetését célozzák, hanem a **magyar szektor ellenállóképességének** a fenyegetettségi kép fejlődési irányához igazított **növelését**.

Bevezetés és módszertan

Az **energiaellátás** minden más **kritikus szolgáltatás** működésének **előfeltétele**, ezért az ágazat elleni kibertámadások következményei messze túlmutatnak az érintett szervezetek keretein. Az elmúlt évtized nemzetközi tapasztalatai azt mutatják, hogy az energetikai infrastruktúra a geopolitikai konfliktusok egyik elsődleges célpontjává vált, miközben **a szektor digitális átalakulása** – a termelés decentralizációjától az ipari vezérlőrendszerek hálózati integrációjáig – folyamatosan bővíti a támadható felületet. Magyarország számára ez a kettős folyamat különös jelentőséggel bír: az ország energiarendszere mélyen beágyazódik a közép-európai regionális infrastruktúrába, ellátási útvonalai geopolitikailag exponált térségeken haladnak keresztül, hazai piacát pedig néhány, rendszerszinten meghatározó szereplő koncentrált működése jellemzi.

A tanulmány célja és hatóköre

A tanulmány célja, hogy a magyar energiaszektor kiberbiztonsági fenyegetettségéről olyan **elemző képet** adjon, amely egyszerre szolgálja a **felsővezetői döntéshozatalt** és a **szakmai közösség helyzetértékelését**. Nem incidenskatalógus és nem megfelelőségi útmutató: a hangsúly annak megértésén van, hogy mely **szereplők**, milyen **motivációval** és milyen **módszerekkel** jelenthetnek **fenyegetést** a hazai energetikai infrastruktúrára, és e fenyegetések miként fejlődhetnek a következő években.

A vizsgálat középpontjában a **villamosenergia-rendszer**, a **földgázinfrastruktúra** és a **távhőszolgáltatás** áll, kitérve a **nukleáris kapacitások** sajátos kockázati profiljára is. A nemzetközi incidensek – köztük

az ukrajnai villamosenergia-rendszer elleni támadások vagy az amerikai csővezeték-üzemeltetőket ért zsarolóvírus-események – nem önmagukban, hanem elemzési referenciaként jelennek meg: azt vizsgáljuk, hogy az ott azonosított képességek és módszerek milyen feltételek mellett érvényesülhetnének a magyar környezetben. A hatókör a **hazai szabályozási** és **intézményi környezetre** is kiterjed, mivel a fenyegetettség értékelése nem választható el attól a védelmi kapacitástól, amelyet az állami és ágazati keretrendszer biztosít.

A tanulmány tudatosan a **stratégiai** és **operatív** elemzési szintre összpontosít. A technikai részletek – konkrét sérülékenységek, indikátorok, detekciós szabályok – kívül esnek a hatókörén, mert ezek gyorsan avulnak, és kezelésük az üzemeltetők napi CTI-folyamatainak feladata. A cél ehelyett az, hogy a döntéshozók a **fenyegetettségi kép** szerkezetét értsék meg, és ebből vezethessék le a saját szervezetükre érvényes prioritásokat.

Elemzési keret és forráskezelés

Az elemzés a CTI szemléletét követi, amely a fenyegetést nem elszigetelt technikai eseményként, hanem **szereplő, szándék, képesség** és **lehetőség** együtteseként értelmezi. Ez a megközelítés teszi lehetővé, hogy a tanulmány ne csupán a már bekövetkezett eseményekből, hanem a szereplők motivációinak és képességfejlődésének irányából következtessen a várható fenyegetésekre. A **fenyegető szereplők tipizálása**, a **támadási módszerek trendelemzése** és az **ágazati kitettség** vizsgálata együttesen adja azt a hármas nézőpontot, amelyből a magyar szektor kockázati profilja felrajzolható.

A forráskezelés terén a tanulmány **kizárólag nyilvánosan elérhető információkra támaszkodik**: nemzetközi CTI-jelentésekre, kormányzati és uniós ügynökségi elemzésekre (különösen az ENISA, a CISA és a nemzeti CERT-szervezetek publikációira), valamint a hazai hatósági és incidenskezelő szervezetek nyilvános közleményeire. A nyílt forrású megközelítésnek módszertani következménye van: a magyar energiaszektort érintő incidensek jelentős része nem válik nyilvánossá, ezért a hazai fenyegetettségi kép szükségszerűen részben a nemzetközi trendek adaptálásán alapul. Ahol a következtetés ilyen extrapoláción nyugszik, a szöveg ezt egyértelműen jelzi.

Az elemzés következetesen elkülöníti a megállapítások három szintjét. **Bizonyított ténynek** a dokumentált, több független forrás által megerősített eseményeket és adatokat tekintjük. **Szakmai következtetésnek** azt, ami a tényekből az ágazat működési logikájának ismeretében megalapozottan levezethető. **Előretekintő értékelésnek**

pedig azt, ami a jelenlegi trendek folytatódását feltételezve valószínűsíthető, de bekövetkezése nem bizonyosság. Ez a hármas megkülönböztetés különösen ott hangsúlyos, ahol – mint a fejlődő technológiák esetében – a dokumentált incidensek száma alacsony.

A magyar energiaszektor mint támadási felület

A fenyegetettség értékelése a **célpont ismeretével** kezdődik. Egy energiarendszer kibertámadásokkal szembeni kitettségét nem elsősorban az alkalmazott védelmi technológiák határozzák meg, hanem a rendszer szerkezete: a **termelés** és az **elosztás koncentráltsága**, a **fizikai** és a **digitális** infrastruktúra **összefonódásának mértéke**, valamint a **külső függőségek jellege**. A magyar energiaszektor e három dimenzió mindegyikében sajátos képet mutat. A rendszer egyszerre erősen koncentrált és gyorsan decentralizálódó, korszerűsödő és jelentős örökölt technológiai állományt hordozó, hazai irányítású és regionálisan mélyen integrált.

A hazai energiarendszer szerkezeti sajátosságai

A magyar **villamosenergia-rendszer** működési szempontból **kevés, rendszerszinten kritikus szereplő köré szerveződik**. Az átviteli hálózat irányítását egyetlen rendszerirányító végzi, a hazai termelés meghatározó hányadát a paksi atomerőmű adja, az elosztást pedig néhány nagy elosztói engedélyes látja el jól lehatárolt területeken. A **földgázszektorban** hasonló a helyzet: az átviteli rendszerüzemeltetés, a stratégiai tárolás és a nagykereskedelem egyaránt koncentrált struktúrában működik. Ez a koncentráció kiberbiztonsági szempontból kettős természetű. Egyfelől lehetővé teszi, hogy a védelmi erőforrások és a szakértelem néhány, jól azonosítható szervezetnél összpontosuljon, ami a nemzetközi tapasztalatok szerint magasabb védelmi érettséget eredményez, mint egy szétaprózott piac. Másfelől viszont azt jelenti, hogy **kisszámú célpont sikeres kompromittálása rendszerszintű következményekkel járhat** – a támadó szemszögéből a magyar energiarendszer „értékes célpontjainak" listája rövid és jól feltérképezhető.

E koncentrált alapszerkezetre az elmúlt években gyors decentralizációs folyamat rakódott. A **naperőművi** kapacitás növekedése – az **ipari** méretű erőművektől a **háztartási** méretű **kiserőművek** százezres nagyságrendjéig – alapvetően alakítja át a termelési oldalt. Rendszerirányítás szempontjából ez azt jelenti, hogy a korábban néhány tucat nagy termelőegység helyett ma

már eszközök tömegének viselkedése befolyásolja a rendszeregyensúlyt, miközben ezen eszközök jelentős része a kritikus infrastruktúra hagyományos védelmi keretein kívül, fogyasztói szintű informatikai környezetben üzemel. A támadási felület így nem egyszerűen nő, hanem jellegében változik: a jól őrzött, kisszámú központi célpont mellett megjelenik egy **heterogén, nehezen felügyelhető peremréteg**, amelynek aggregált manipulációja elvben rendszerszintű hatást érhet el. E szerkezeti átalakulás következménye, hogy a magyar rendszer kitettsége ma már nem írható le pusztán a nagy üzemeltetők biztonsági szintjével.

A **távhőszektor** a harmadik jellegzetes réteg. A hazai távhőszolgáltatás jellemzően önkormányzati tulajdonú, lokálisan szervezett vállalatokra épül, amelyek erőforrásai és kiberbiztonsági érettsége jelentősen elmarad a nagy energetikai társaságokétól, miközben szolgáltatásuk kiesése – különösen a fűtési idényben – közvetlen és gyorsan eszkalálódó társadalmi hatással jár. A fenyegető szereplők szempontjából az ilyen aszimmetria vonzó: a távhőszolgáltatók a szektor **legkisebb ellenállású** pontjai közé tartoznak, amit a régió más országaiban dokumentált, fűtési rendszereket érintő incidensek — a lvivi és a lengyelországi eset — is alátámasztanak. A magyar energiaszektor támadási felülete tehát nem homogén, hanem **érettségi szintek szerint erősen rétegzett** – és a támadók jellemzően nem a legerősebb, hanem a leggyengébb réteghez igazítják a belépési pontjukat.

Az IT/OT konvergencia és az örökölt rendszerek

Az energetikai infrastruktúra digitális gerincét az **operatív technológiai** (OT) rendszerek adják: a **folyamatirányító** és **felügyeleti** rendszerek, az **alállomási automatika**, a **védelmi berendezések** és a **telemechanikai hálózatok**. Ezek a rendszerek évtizedekig fizikailag és logikailag elkülönülten működtek a vállalati informatikától, ami önmagában is védelmi funkciót töltött be. Az elmúlt tizenöt év fejlődése – a távoli üzemeltetés igénye, az adatalapú karbantartás, a piaci adatszolgáltatási kötelezettségek és az energiahatékonysági optimalizálás – ezt az elkülönülést fokozatosan felszámolta. A konvergencia üzemeltetési szempontból racionális és visszafordíthatatlan folyamat, kiberbiztonsági szempontból azonban azt eredményezi, hogy **a vállalati IT-környezet kompromittálása potenciális kiindulópontjává válik a fizikai folyamatok elleni támadásnak**.

A magyar szektorban ez a konvergencia egy sajátos technológiai örökséggel találkozik. Az ipari vezérlőrendszerek beruházási ciklusa évtizedes léptékű: a ma üzemelő alállomási és folyamatirányítási eszközpark jelentős része olyan korszakból származik, amikor a hálózati kitettség nem volt tervezési szempont. Ezek az eszközök gyakran nem támogatnak hitelesítést vagy

titkosított kommunikációt, gyártói támogatásuk lejárt, cseréjük pedig üzembiztonsági és költségokokból csak lassan halad. A nemzetközi CTI-elemzések visszatérő megállapítása, hogy az energetikai OT-környezetek elleni sikeres támadásokhoz jellemzően **nem szükséges kifinomult sérülékenység-kihasználás**: a rendszerek dokumentált, szabványos funkcióinak rosszindulatú használata – tehát a mérnöki protokollok rendeltetésszerű, de jogosulatlan alkalmazása – önmagában elegendő a fizikai folyamatok befolyásolásához. Ez a felismerés a védelem súlypontját a sérülékenységmenedzsmentről a hozzáférés-kontroll, a szegmentáció és az anomáliadetektálás irányába tolja el, aminek a hazai üzemeltetőkre nézve közvetlen következményei vannak.

Külön figyelmet érdemel az ellátási lánc digitális dimenziója. A hazai energetikai társaságok OT-rendszereinek szállítói, integrátorai és karbantartói túlnyomórészt nemzetközi gyártók és azok hazai partnerei; a távoli gyártói hozzáférés, a karbantartói VPN-kapcsolatok és a rendszerintegrátori jogosultságok **olyan bizalmi csatornákat képeznek, amelyek a célszervezet védelmi rendszerein kívül esnek**, mégis közvetlen utat nyithatnak a folyamatirányításig. A nemzetközi incidensek tapasztalata szerint a fejlett szereplők előszeretettel választják ezt az utat, mert a beszállítói kapcsolat legitimitása elfedi a behatolást. A magyar szektor beszállítói hálózata méreténél fogva áttekinthetőbb, mint a nagy nyugat-európai piacoké, ez azonban a védelmet csak akkor szolgálja, ha a bizalmi kapcsolatok tényleges felügyelet alá kerülnek – e feltétel teljesülése ma szervezetenként igen eltérő.

Regionális összekapcsoltság és ellátási függőségek

A **magyar energiarendszer** nem önálló egységként, hanem a **közép-európai infrastruktúra csomópontjaként** működik. A villamosenergia-hálózat szinkronüzemben kapcsolódik a kontinentális európai rendszerhez, a határkeresztező kapacitások az ország villamosenergia-fogyasztásának jelentős hányadát fedező importot bonyolítanak, a földgázhálózat pedig egyszerre szolgálja a hazai ellátást és a regionális tranzitot. Ez az integráció ellátásbiztonsági szempontból erőforrásmegosztási kérdés, kiberbiztonsági szempontból azonban azt jelenti, hogy **a magyar rendszer kitettsége nem ér véget az országhatárnál**. A szomszédos rendszerirányítók, a közös európai piaci platformok és az adatcsere-infrastruktúrák elleni támadások közvetve a hazai rendszer működését is érinthetik, miközben ezekre a hazai szereplőknek korlátozott a ráhatásuk.

A tranzitszerep önálló kockázati tényező. Az országon áthaladó földgáz- és kőolajvezetékek, valamint a délkeleti irányú gázszállítási útvonal regionális jelentősége a magyar infrastruktúrát olyan szereplők látókörébe is emeli, amelyek célja nem Magyarország, hanem a tágabb európai ellátási rendszer befolyásolása. A **geopolitikai feszültségek** időszakában –az orosz–ukrán háború óta tartósan ilyen időszakban élünk – a tranzitinfrastruktúra a nyomásgyakorlás és a jelzésértékű műveletek természetes terepe. A jelenlegi nyilvános CTI-információk alapján a magyar tranzitinfrastruktúra ellen célzott, romboló szándékú kiberművelet nem dokumentált; a nemzetközi trendek – különösen az európai energetikai szervezetek elleni felderítő jellegű, előpozicionálást szolgáló kampányok – alapján azonban megalapozottan feltételezhető, hogy a magyar rendszerek e szereplők felderítési tevékenységének tárgyát képezik.

A függőségek harmadik rétege **technológiai** természetű. A hazai energetikai rendszerek irányítástechnikája, piaci informatikája és egyre nagyobb mértékben felhőalapú szolgáltatási környezete néhány nemzetközi technológiai szállító termékeire épül. Ez a globális iparági norma, következménye azonban az, hogy egy-egy széles körben használt platform sérülékenysége vagy kompromittálása egyszerre több hazai kritikus szereplőt érinthet – **a kockázat tehát korrelált, nem pedig szervezetenként független**.

A nukleáris kapacitások sajátos kockázati profilja

A paksi atomerőmű a magyar villamosenergia-termelés meghatározó szereplője, kockázati profilja azonban jelentősen eltér az energiaszektor más elemeitől. Ennek hátterében a nukleáris biztonság és a kiberbiztonság szoros összefonódása, a létesítményre vonatkozó kiemelten szigorú szabályozási környezet, valamint egy esetleges sikeres kibertámadás sajátos következményei állnak. Míg az energiaszektor más területein a kibertámadások hatása elsősorban az üzem- és ellátásbiztonságot veszélyeztetheti, egy nukleáris létesítmény esetében a következmények a nukleáris biztonságot is érinthetik. A fokozott szabályozás, a többszintű védelmi követelmények és a biztonságkritikus rendszerek sajátosságai miatt a nukleáris terület a hazai energiaszektor egyik legmagasabb biztonsági érettségű rétegét képviseli.

A nukleáris kockázati profil megkülönböztető vonása mindenekelőtt a **biztonságkritikus** (safety) és a **biztonságvédelmi** (security) rendszerek szigorú, tervezési szintre visszavezetett **elkülönítése**. Míg a szektor többi részében az IT és az OT konvergenciája fokozatosan felszámolta a rendszerek közötti határokat, a nukleáris létesítményekben ezt az

elkülönítést a szabályozás kifejezetten fenntartja és kikényszeríti. A hazai keret gerincét az atomenergiáról szóló 1996. évi CXVI. törvény, az atomenergia alkalmazása körében a fizikai védelemről szóló 190/2011. Korm. rendelet, valamint a nukleáris létesítmények nukleáris biztonsági követelményeiről szóló 1/2022. OAH rendelet adja. E keret két olyan alapelvet rögzít, amely a szektor többi részének szabályozásából hiányzik. Az egyik a **tervezési alapfenyegetettség** fogalma: a védelmet nem általános kockázatokhoz, hanem egy explicit módon meghatározott, feltételezett támadói képességszinthez kell méretezni. A másik a **programozható rendszerek** kötelező, **biztonsági osztályokba és védelmi zónákba sorolása**, azzal a kikényszerített megkötéssel, hogy alacsonyabb biztonsági osztályba sorolt rendszer nem befolyásolhatja a magasabb osztályba sorolt rendszer működését. Ez a zónamodell rokon ugyan az OT-környezetekben általánosan alkalmazott szegmentációs logikával, annál azonban lényegesen szigorúbb: nem ajánlott jó gyakorlat, hanem hatóságilag felügyelt, engedélyezési feltételként számonkért követelmény. Szakmai következtetésként megfogalmazható, hogy a nukleáris réteg éppen ezért mentes a szektor más rétegeit jellemző legfőbb strukturális gyengeségektől – az örökölt, védelem nélküli eszközparktól és a felügyelet nélküli bizalmi hozzáférésektől –, mivel ezeket a szabályozás tervezési szinten kizárja.

A nukleáris létesítmények elleni, dokumentált kiberincidensek nemzetközi tapasztalata két, egymást kiegészítő tanulságot kínál. Az első az opportunista, nem célzott fenyegetés kockázata: a 2003-as Davis-Besse-eset, amelyben a Slammer-féreg egy amerikai atomerőmű vállalati hálózatán keresztül elérhetetlenné tette a biztonsági paraméterek megjelenítő rendszerét (Safety Parameter Display System) csaknem öt órára, azt mutatja meg, hogy a nukleáris safety-rendszerek sem sérthetetlenek egy egyszerű, nem is nekik szánt kártevővel szemben. A második, súlyosabb tanulságot a 2010-ben felfedezett Stuxnet adja, amely az iráni natanzi urándúsító centrifugái ellen irányult: az eset bizonyította, hogy egy kellően felkészült állami szereplő még a fizikailag izolált, az internetről leválasztott (air-gapped) nukleáris környezetbe is képes bejuttatni célzott kártevőt – jellemzően a beszállítói lánc vagy egy adathordozó közvetítésével –, és fizikai károkozásig eljutni úgy, hogy közben az operátorok felé a rendszer normál működést jelez. A Stuxnet ezért a nukleáris kontextus emblematikus figyelmeztetése: **az air-gap fontos, de nem elégséges védelem**, és hamis biztonságérzetet kelthet, ha a szegmentáció és a bizalmi csatornák felügyelete nem egészíti ki.

E nemzetközi tapasztalatok magyar vonatkozású értékelése óvatosságot igényel, és a bizonyossági szintek szigorú elkülönítését. **Bizonyított ténynek**

az tekinthető, hogy a hazai nukleáris szabályozási keret a nemzetközi jó gyakorlatnak megfelelő, kikényszerített védelmi követelményeket ír elő, és hogy a paksi kapacitás rendszerszinten kritikus. Szakmai következtetésként megfogalmazható, hogy e szabályozási rezsim a nukleáris réteget a szektor legjobban védett elemévé teszi, így a rá irányuló, sikeres fizikai károkozás valószínűsége lényegesen alacsonyabb, mint a gyengébben felügyelt rétegeké – a Stuxnet tanulsága szerint azonban ez a képesség a legfelkészültebb állami szereplők szűk körénél nem zárható ki teljesen. Előretekintő értékelésként pedig az emelhető ki, hogy a Paks II. beruházás a nukleáris kiberbiztonság szempontjából **egyszerre kockázat és lehetőség**: egy új létesítmény tervezése az egyetlen olyan pillanat, amikor a biztonsági architektúra a legkorszerűbb elvek szerint, örökölt technológiai teher nélkül alakítható ki – feltéve, hogy a kiberbiztonsági és beszállítói-lánc szempontok már a tervezési fázisban, nem utólagos ráépítésként érvényesülnek. A nukleáris réteg tehát a fenyegetettségi kép sajátos szegletét képviseli: itt nem a védelmi képesség hiánya, hanem a legfelkészültebb szereplőkkel szembeni maradékkockázat és a beruházási döntések hosszú távú hatása a mérlegelés tárgya.

Fenyegető szereplők és motivációk

A támadási felület önmagában csak lehetőség; fenyegetéssé attól válik, hogy léteznek szereplők, amelyeknek szándékában és képességében áll kihasználni. A kulcskérdés ezért az, hogy ki, milyen célból és milyen erőforrásokkal tekinthet célpontként a magyar energiaszektorra. A nemzetközi tapasztalat szerint az energetikát fenyegető szereplői kör négy, egymástól motivációban és képességszintben jól elkülönülő csoportra osztható: az államilag támogatott szereplőkre, a haszonszerzés-vezérelt kiberbűnözésre, az ideológiai indíttatású hacktivizmusra és a belső fenyegetésre. E kategóriák határai a gyakorlatban egyre gyakrabban elmosódnak – éppen ez az elmosódás a fenyegetettségi kép egyik legfontosabb újdonsága –, elemzési kiindulópontként azonban továbbra is ez a felosztás ad használható szerkezetet.

Ezt a nemzetközi felosztást egy hazai, kifejezetten a villamosenergia-szektorra kidolgozott osztályozási keret is megerősíti. A SeConSys szakmai együttműködés keretében, az NBSZ - NKI gondozásában kiadott ágazati kézikönyv a támadókat négy dimenzió – a motiváció, az információszerzési képesség mélysége, a technikai tudásszint és a rendelkezésre álló erőforrások mennyisége – mentén sorolja kategóriákba, a legkevesebb erőforrással rendelkező, kész eszközöket használó alkalmi támadótól a belső

munkatárson, beszállítón, hacktivista csoportokon és kiberbűnözőkön át a legnagyobb erőforrású, államilag támogatott csoportokig. A hazai keret ugyanakkor arra is emlékeztet, hogy a nagy nyilvánosságot kapó állami és zsarolóvírusos fenyegetések mellett az alacsony képességű, opportunista támadó és a bizalmi körből érkező belső szereplő is állandó eleme a fenyegetettségi képnek.

Államilag támogatott szereplők

Az energetikai infrastruktúra elleni legsúlyosabb, fizikai hatást célzó műveletek eddig **kivétel nélkül állami hátterű szereplőkhöz köthetők**. A dokumentált esetek sora Ukrajnából ismert: a 2015-ös áramkimaradást okozó, BlackEnergy kártevőhöz kötött művelet, a 2016-os, kijevi alállomást érintő Industroyer-támadás, majd a 2022-ben, már a háború alatt azonosított Industroyer2-kísérlet egyaránt az orosz katonai hírszerzéshez kötött Sandworm csoport tevékenységeként vált ismertté a CERT-UA és az ESET elemzései nyomán. Ezek az esetek két okból meghatározóak a magyar helyzetértékelés szempontjából. Egyrészt bizonyítják, hogy a villamosenergia-rendszer elleni, fizikai következménnyel járó kibertámadás nem elméleti lehetőség, hanem **többször végrehajtott képesség**. Másrészt megmutatják e képesség korlátait is: a műveletek hosszú előkészítést igényeltek, hatásuk órákban-napokban volt mérhető, és a helyreállítást a manuális üzemvitel képessége minden esetben lehetővé tette.

Az állami szereplők fizikai károkozási képessége nem csupán a valós incidensekből, hanem **kontrollált kísérletből** is dokumentált. A 2007-ben az Idaho National Laboratories által végrehajtott kísérlet – a később Aurora néven ismertté vált teszt – igazolta azt az addig hipotézisként kezelt feltevést, hogy pusztán **kiberbiztonsági beavatkozásból** is származhat **fizikai károkozás**: a kísérletben egy generátor védelmi reléjének jogosulatlan vezérlésével, a megszakítók fázison kívüli, ismételt nyitásával és zárásával idéztek elő helyrehozhatatlan fizikai károsodást. E kísérlet azért fontos viszonyítási pont, mert megmutatja, hogy a fizikai rombolás képessége nem az egyes kártevők tulajdonsága, hanem a vezérlőrendszerekhez való jogosulatlan hozzáférés önmagában is elegendő feltétele lehet.

A magyar szektor szempontjából azonban **nem a rombolás a legvalószínűbb állami tevékenységi forma, hanem az előpozicionálás**: a hálózatokba való csendes behatolás és a hozzáférés fenntartása egy későbbi, politikai döntéstől függő aktiválás céljából. Ezt a mintázatot a nyugati hatósági jelentések következetesen dokumentálják – az amerikai kormányzat 2018-ban hozta nyilvánosságra az orosz állami szereplők

energetikai célú, több éven át tartó felderítő kampányát, a CISA 2024-es riasztása pedig a kínai Volt Typhoon csoport kritikus infrastruktúrákban való, kifejezetten a későbbi zavarkeltést előkészítő jelenlétét írta le. Az **előpozicionálás** jellegéből fakad, hogy jelenléte ritkán válik nyilvánossá; a jelenlegi nyilvános CTI-információk alapján magyar energetikai rendszerekben ilyen tevékenység nem dokumentált, a nemzetközi trendek és Magyarország regionális szerepe alapján azonban szakmai következtetésként megfogalmazható, hogy a hazai szektor e szereplők felderítési célrendszerében szerepel. A védelmi tervezésnek ezért nem abból kell kiindulnia, hogy történik-e ilyen kísérlet, hanem abból, hogy a **felderítés** és a **tényleges károkozás** közötti hosszú szakasz a védekező számára is **időt ad** – ha rendelkezik az észleléséhez szükséges képességekkel.
Az állami szereplők motivációs logikája végül geopolitikai természetű, és ez adja az értékelés dinamikáját. Az energetikai célpontok elleni műveleti aktivitás a nemzetközi tapasztalat szerint nem folyamatos, hanem a politikai feszültségek függvényében hullámzik; eszkalációs időszakban a korábban kiépített hozzáférések felértékelődnek. A magyar fenyegetettségi szint tehát **nem állandó,** hanem az **európai biztonsági környezet alakulásával együtt mozog**.

A kiberbűnözői ökoszisztéma és a zsarolóvírus-fenyegetés

Miközben a legnagyobb potenciális kárt az állami szereplők képviselik, **a ténylegesen realizált károk túlnyomó részét világszerte a haszonszerzés-vezérelt kiberbűnözés okozza**, és ez a magyar szektorra is érvényes kiindulópont. A 2022 és 2024 közötti globális energetikai kiberincidensek szisztematikus elemzése ezt kvantitatívan is megerősíti: a **pénzügyi motivációjú incidensek** adták a legnagyobb csoportot, a **domináns támadástípus a zsarolóvírus** volt, a leginkább **érintett térségek** között pedig az **Európai Unió** az élmezőnyben szerepelt. A **zsarolóvírus-műveletek** az elmúlt években **iparszerű szolgáltatási modellé szerveződtek**: a kártevőfejlesztés, a kezdeti hozzáférés megszerzése és a zsarolás lebonyolítása egymástól elváló, piaci alapon működő szerepekre bomlott. Ennek a munkamegosztásnak a célpontkiválasztásra nézve fontos következménye van: a kezdeti hozzáféréssel kereskedő szereplők nem ágazat szerint válogatnak, hanem opportunista módon, a sérülékeny rendszerek alapján – egy energetikai vállalat tehát **nem azért válik áldozattá, mert energetikai, hanem mert elérhető volt**. Az ágazati jelleg a folyamat második szakaszában, a váltságdíj meghatározásánál értékelődik

fel, mivel a szolgáltatáskiesés társadalmi költsége növeli a fizetési hajlandóságra vonatkozó támadói várakozást.
Az energetikai relevancia szempontjából a 2021-es Colonial Pipeline eset maradt a viszonyítási pont: a DarkSide csoport támadása az üzemeltető informatikai rendszereit érintette, az üzemanyag-szállítás napokig tartó leállítása mégis bekövetkezett, mert a vállalat az OT-környezet érintettségének kizárásáig nem vállalta az üzemeltetés folytatását. Az eset általánosítható tanulsága, hogy **a zsarolóvírusnak nem kell elérnie a folyamatirányítást ahhoz, hogy fizikai szolgáltatáskiesést okozzon** – elegendő a bizonytalanság, amelyet az IT- és OT-környezet elégtelen szétválasztása kelt. A hazai szektor rétegzett érettségi képe itt válik közvetlenül kockázattá: a nagy üzemeltetőknél a szétválasztás jellemzően kezelt kérdés, a távhőszolgáltatói és beszállítói rétegben azonban a nemzetközi mintázat alapján reális az a forgatókönyv, hogy egy opportunista zsarolóvírus-incidens szolgáltatáskiesésig eszkalálódik.
Ezt a forgatókönyvet egy közvetlen szomszédos, energetikai eset frissen is szemlélteti: a román Electrica Group elleni, 2024. decemberi zsarolóvírus-támadás. A mintegy 3,8 millió felhasználót ellátó, országosan meghatározó áramszolgáltatónál az elkövetőként azonosított Lynx-csoport ellenére a kritikus SCADA- és egyéb üzemirányítási rendszereket idejében leválasztották, így azok érintetlenek maradtak, az áramellátás pedig folyamatos maradt. Az eset a Colonial Pipeline energetika-specifikus, regionális párja: megerősíti, hogy egy IT-oldali zsarolóvírus-incidens az **OT-környezet izolációja** révén tartható távol a fizikai szolgáltatástól – földrajzi közelsége és frissessége pedig a hazai értékelés különösen erős viszonyítási pontjává teszi.
A zsarolóvírus-aktivitás évek óta a hazai fenyegetettségi kép egyik meghatározó eleme; energetikai szereplőt érintő, nyilvánosan megerősített hazai súlyos eset ugyanakkor nem ismert, ami a nemzetközi bázisráták fényében részben a nyilvánosságra kerülés hiányával magyarázható, nem a fenyegetés hiányával.
Az ökoszisztéma és az állami szféra közötti határ egyes joghatóságokban átjárható. A zsarolóvírus-csoportok egy része bizonyíthatóan olyan környezetben működik, amely tevékenységüket eltűri vagy irányítottan hasznosítja, így **a haszonszerzési és a geopolitikai motiváció nem zárja ki egymást**. A védekező szempontjából ennek gyakorlati jelentése az, hogy a „bűnözői” incidens sem kezelhető automatikusan alacsonyabb kategóriaként – a hozzáférés, amelyet egy zsarolóvírus-művelet épít ki, más célra is továbbadható.

Hacktivizmus és a láthatóságért folytatott műveletek

A harmadik szereplői réteg az ideológiai indíttatású, nyilvánosságorientált tevékenység, amely az orosz–ukrán háború kitörése óta Európa-szerte; a politikai motivációjú támadásokon belül a hacktivizmus vált a leggyakoribb kategóriává, elsősorban a villamosenergia-alszektort célozva. A pro-orosz hacktivista csoportok – köztük a NoName057(16) és a KillNet néven ismert hálózatok – működésének jellegzetes formája az elosztott túlterheléses támadás, amelynek célpontjait a napi politikai események alapján, demonstratív céllal választják ki. Magyarországi célpontok elleni ilyen kampányokról az elmúlt években több alkalommal jelentek meg nyilvános beszámolók, azonban nem az energiaszektort, hanem főként kormányzati és pénzügyi webes felületeket célozva. A műveletek technikai hatása korlátozott volt: publikus felületek ideiglenes elérhetetlenségét okozták, a folyamatirányítást nem érintették.

A hacktivista fenyegetés jelentőségét ezért **nem a közvetlen kárpotenciál adja, hanem két közvetett mechanizmus**. Az első a **kommunikációs hatás**: az energetikai szereplő elleni látványos, még ha technikailag felszínes támadás is alkalmas a szolgáltatásba vetett bizalom gyengítésére, különösen ellátási feszültségek időszakában – a hacktivizmus ebben az értelemben a befolyásolási műveletek olcsó eszköze. A második az **eszkalációs mechanizmus**: a nemzetközi CTI-jelentések az utóbbi években olyan csoportokat is dokumentáltak, amelyek hacktivista arculat mögött ipari vezérlőrendszerek elleni, kezdetleges, de valós beavatkozási kísérleteket hajtottak végre, jellemzően internetre kitett, gyenge hitelesítésű eszközök ellen. Ezek a kísérletek **képességszintben messze elmaradnak** az állami műveletektől, ugyanakkor pontosan azt a heterogén, gyengén felügyelt **peremréteget célozzák**, amely a magyar rendszer **legkevésbé ellenálló eleme**. A hacktivizmus tehát elsősorban nem szofisztikáltsága, hanem **célpontválasztási logikája miatt érdemel figyelmet** a hazai értékelésben.

A hacktivista tevékenység súlyát a **hibrid fenyegetés** összefüggésében nyeri el. Az **energiaszektor** azért kerülhet e **műveletek középpontjába**, mert **minden más kritikus ágazat működésének előfeltétele**, egy összehangolt művelet végső célja pedig gyakran nem közvetlenül a fizikai kár, hanem a **lakosság államigazgatás iránti bizalmának rombolása**, ezáltal az ellenállóképesség gyengítése. A 2015-ös ukrajnai támadássorozat épp ezt a pszichológiai dimenziót példázza: a támadók a hálózat megbénításával párhuzamosan a szolgáltatói ügyfélszolgálati központokat

is elérhetetlenné tették, hogy a fogyasztók se tudjanak tájékozódni, 2016-ban pedig a kezelőszemélyzet szándékos hibára kényszerítésének kísérletével fokozták a hatást. A hibrid fenyegetéssel szemben ugyanakkor a regionális összekapcsoltság védelmi tényezőként is működik: a hazai átviteli hálózat ENTSO-E-integrációja csökkenti egy esetleges dominóhatás következményeit – ez a kétélű összekapcsoltság védelmi oldala.

Belső fenyegetés és a bizalmi kapcsolatok kockázata

A negyedik réteg a szervezeten belülről vagy a bizalmi körből származó fenyegetés, amely a nyilvános elemzésekben rendszerint alulreprezentált, mert az ilyen esetek ritkán kerülnek nyilvánosságra. Az energetikai környezetben a belső fenyegetés súlyát az adja, hogy **a jogosult hozzáférés megkerüli a védelmi architektúra külső támadó ellen épített rétegeit**: egy üzemviteli jogosultsággal rendelkező munkatárs vagy karbantartó partner számára a folyamatirányítás elérése nem behatolási feladat, hanem munkaköri adottság. A belső szereplő emellett a külső támadónál lényegesen több információval rendelkezik: nemcsak magát a rendszert, hanem annak gyengeségeit és a szervezet biztonsági eljárásrendjét is ismeri. A kockázat mindazonáltal nem elsősorban a rosszindulatú szándékból fakad – ennek dokumentált előfordulása alacsony –, hanem a jogosultságok gondatlan kezeléséből, a megosztott technológiai fiókokból és a kilépő munkatársak vissza nem vont hozzáféréseiből, amelyek külső szereplő számára is felhasználható belépési pontot képeznek.

Hogy ez a kockázat mennyire kézzelfogható, egy regionális, energetikai eset is mutatja: a szlovén Holding Slovenske Elektrarne (HSE) elleni, 2023. novemberi Rhysida-támadás. Az ország legnagyobb, a hazai villamosenergia-termelés mintegy 60%-át adó termelőjénél – amelynek több más ország mellett magyarországi leányvállalata is van – a kártevő a fájlokat titkosította, az áramtermelést azonban nem zavarta meg. A behatolás gyökere a nyilvános beszámolók szerint nem kifinomult támadói képesség, hanem **gyenge kiberhigiénia** volt: egy védtelen felhőtárolóban tárolt jelszókészlet – vagyis pontosan a jogosultságok gondatlan kezelése, amely külső szereplő számára is nyitva hagyja a bizalmi belépési pontot.

A belső dimenzió a magyar szektorban két okból kap külön hangsúlyt. Az egyik a munkaerőpiaci helyzet: az OT-üzemeltetési és irányítástechnikai szaktudás szűkös, a kulcskompetenciák kevés személyben összpontosulnak, ami egyszerre növeli e személyek célértékét a social engineering műveletek számára és nehezíti a feladatkörök szétválasztásán alapuló kontrollok bevezetését. A másik a korábban már elemzett beszállítói

szerkezet: a karbantartói és integrátori hozzáférések a gyakorlatban **a belső jogosultságokkal egyenértékűek**, miközben a felettük gyakorolt munkáltatói és biztonsági kontroll a célszervezeten kívül esik. E kategória a beszállítói lánc felől érkező támadásokat is magában foglalja, amelyek nem feltétlenül a beszállító szándékos közreműködésével valósulnak meg: egy külső támadó a beszállító rendszerét kompromittálva, annak legitim jogosultságaival hajthat végre műveleteket a végső célpont ellen. Ez a mechanizmus a nukleáris kontextusban is ismert: a Stuxnet tanulsága szerint éppen a beszállítói vagy adathordozós közvetítés jelentette a fizikailag izolált környezetbe való bejutás útját.

Támadási módszerek és trendek

A szereplők ismerete akkor válik operatívan hasznossá, ha megértjük, milyen módszerekkel dolgoznak, és e módszerek milyen irányba fejlődnek. A nemzetközi incidensekből kirajzolódó módszertani mintázatok a magyar szektor szerkezeti adottságai mellett nyerik el valódi jelentésüket. A hangsúly nem az egyes esetek technikai rekonstrukcióján van, hanem azon, hogy mely támadási minták bizonyultak tartósnak, melyek terjednek, és melyek illeszkednek különösen jól a hazai kitettségi képhez.

A kezdeti hozzáférés útvonalai

A támadási életciklus legköltségesebb és a védekező számára leginkább befolyásolható szakasza a kezdeti hozzáférés megszerzése. A nemzetközi incidenselemzések visszatérő megállapítása, hogy az energetikai szereplők elleni behatolások ritkán indulnak a folyamatirányítási rendszer közvetlen ostromával; **a belépési pont jellemzően a vállalati informatikai környezet**, ahonnan a támadó fokozatosan, oldalirányú mozgással közelít az operatív technológia felé. A leggyakoribb kiindulóvektorok – az adathalászat, a nyilvános szolgáltatások sérülékenységeinek kihasználása és a kompromittált hitelesítő adatok – nem energetika-specifikusak, éppen ez teszi az energetikai szervezeteket is elérhetővé az opportunista szereplők számára. A bűnözői munkamegosztás így technikai szinten is tetten érhető: a kezdeti hozzáférés megszerzése önálló, iparágtól független tevékenységgé vált.

A magyar szektor szempontjából **a bizalmi csatornákon keresztüli hozzáférés emelkedik ki** a lehetséges útvonalak közül. A beszállítói és karbantartói kapcsolatok a támadási felület sajátos, a célszervezet közvetlen kontrollján kívül eső elemei; a módszertani trendek ezt a strukturális kockázatot konkrét támadói gyakorlattá fordítják. A nemzetközi tapasztalat

szerint a fejlett szereplők tudatosan keresik a beszállítói kompromittálás lehetőségét, mert a legitim karbantartói kapcsolat elfedi a behatolást és megkerüli a peremvédelmet. Az ilyen műveletek nem feltétlenül igényelnek nagy erőforrást: egy kevésbé védett integrátor vagy egy megosztott távoli hozzáférési megoldás kompromittálása **egyszerre több energetikai ügyfélhez nyithat utat**. A hazai szektor áttekinthetőbb beszállítói szerkezete elvben kedvez a felügyeletnek, a gyakorlatban azonban a bizalmi kapcsolatok tényleges monitorozása a hazai üzemeltetőknél egyenetlenül megoldott, ami a kezdeti hozzáférés e vektorát a fenyegetettségi kép egyik alulkezelt elemévé teszi.

A beszállítói-lánc kompromittálás kockázatát a 2020-ban felfedezett SolarWinds/SUNBURST-eset szemlélteti a legélesebben: a támadók egy széles körben használt hálózatfelügyeleti szoftver frissítési mechanizmusába juttattak be hátsó kaput, amely így a gyártó legitim szoftverfrissítésével együtt, megbízhatónak tekintett csatornán jutott el egyszerre több ezer szervezethez világszerte. Az eset megmutatja, hogy a beszállítói-lánc támadás nem szükségszerűen egyetlen célszervezet ellen irányul, hanem egy közösen használt terméken keresztül egyszerre sok üzemeltetőt érinthet – ami közvetlenül összecseng a néhány közös technológiai szállítótól való korrelált függés kockázatával. Ugyanakkor rávilágít arra is, hogy **a legitim frissítési csatorna megbízhatósága önmagában nem garancia**: a beszállítói szoftverek és a rajtuk keresztül érkező frissítések integritásának ellenőrzése a hazai üzemeltetők számára is a hozzáférés-felügyelet szerves részévé kell váljon, nem pedig a beszállítóba vetett bizalomra hagyatkozó, ellenőrzés nélküli folyamat.

A fizikai hatás elérésének logikája

Az energetikai támadások megkülönböztető vonása, hogy **a végső cél nem az adat, hanem a fizikai folyamat befolyásolása**. Az ide vezető módszertan fejlődése tanulságos ívet rajzol ki. A korai, fizikai hatást elérő műveletek – mindenekelőtt a 2016-os Industroyer – célzottan az ipari kommunikációs protokollokra épített kártevőt alkalmaztak, amely önállóan volt képes az alállomási berendezések vezérlésére. Ez a megközelítés jelentős mérnöki ráfordítást igényelt, mert a kártevőt a célkörnyezet protokolljaira kellett szabni. A 2022-es Industroyer2 ugyanezt a logikát vitte tovább, immár a háborús kontextusban egy konkrét ukrán alállomás ellen; a támadást sikerült a hatás bekövetkezése előtt megszakítani, ami maga is fontos tanulság a detekció és a beavatkozás értékéről.

Az Industroyer esete egy másik, gyakran alulértékelt módszertani tanulságot is hordoz. A szakmai elemzések rámutatnak, hogy a 2016-os

művelet nem merült ki a fogyasztói leágazások kikapcsolásában: a támadók a Siemens SIPROTEC alállomási védelmi berendezések egy ismert sérülékenységét kihasználva azok szolgáltatásmegtagadásos kiiktatására is kísérletet tettek. E kettős logika – az üzemzavar előidézése, majd a védelmi berendezések egyidejű kiiktatása – célja egy sokkal pusztítóbb, akár hónapokig-évekig tartó helyreállítást igénylő károkozás előkészítése lehetett, amely csak a támadói kód hibája miatt nem következett be. E tanulság a magyar értékelés szempontjából azt húzza alá, hogy a fejlett OT-támadás nem egyetlen beavatkozás, hanem a biztonsági és védelmi funkciók módszeres, egymásra épülő felszámolása – ezért a védelmi berendezések és a távoli elérési felületek (például a szünetmentes tápellátás távfelügyeleti interfészei) önálló, kiemelt védelmet igényelnek, nem csupán a folyamatirányítás.

A trend azonban a specializált kártevőktől **a rendszer saját, legitim eszközeinek felhasználása felé mozdul**. A „living off the land” megközelítés lényege, hogy a támadó a célkörnyezetben már jelen lévő, jogszerű adminisztrációs és mérnöki eszközöket használja céljai elérésére, egyedi kártevő telepítése helyett. Ez a módszer az energetikai OT-környezetben különösen hatékony, mert a vezérlőrendszerek jelentős része dokumentált, szabványos funkciókkal rendelkezik, amelyek rendeltetésszerű, de jogosulatlan használata önmagában elegendő a folyamatok befolyásolásához. A CISA 2024-es, Volt Typhoonhoz kötött riasztása éppen ezt a mintázatot emelte ki: a hozzáférés fenntartása és a mozgás úgy zajlott, hogy a tevékenység a legitim rendszerhasználattól nehezen volt megkülönböztethető. A védekező szempontjából ennek súlyos következménye van: a fenyegetés jelentős része nem azonosítható kártékony kód jelenlétével, csak a rendszer viselkedésének anomáliáiból, ami **az anomáliaalapú detektálást a hazai OT-védelem kulcsképességévé teszi**.

E módszertani elmozdulás egyúttal árnyalja a fenyegetés súlyosságáról alkotott képet. A rendszer saját eszközeivel végrehajtott beavatkozás technikailag könnyebben kivitelezhető, mint egy egyedi ipari kártevő fejlesztése, hatóköre azonban jellemzően korlátozottabb, és mélyebb rendszerismeretet igényel a célzott, tartós károkozáshoz. A magyar rendszer szempontjából ez azt jelenti, hogy a felszínes, opportunista beavatkozás valószínűsége nő, a nagy léptékű, tervezett rombolás képessége viszont továbbra is a legfelkészültebb állami szereplők szűk körére korlátozódik.

A hozzáférés és a hatás időbeli szétválása

A harmadik, egyre határozottabb trend **a behatolás és a tényleges károkozás időbeli elválása**. Az előpozicionálás módszertani vetülete az, hogy **a hozzáférés megszerzése és fenntartása önálló műveleti céllá vált**, függetlenül attól, hogy a hatás valaha bekövetkezik-e. Ez a mintázat a védekezés egész logikáját átalakítja: a fenyegetés **nem egy jövőbeli esemény, amelyet meg kell előzni, hanem egy jelen idejű állapot, amelyet fel kell deríteni**. A nemzetközi hatósági jelentések kifejezetten arra figyelmeztetnek, hogy a kritikus infrastruktúrákban észlelt behatolások egy része nem azonnali haszonszerzést vagy adatlopást szolgál, hanem egy eszkalációs helyzetben aktiválható képesség előkészítését.

A fenyegetettség értékelésénél a hangsúlyt a megelőzésről a folyamatos észlelés és a hozzáférés-felderítés felé kell tolni, mert egy csendben fenntartott hozzáférés hónapokig-évekig észrevétlen maradhat a hagyományos, eseményvezérelt biztonsági megközelítés számára. A geopolitikai dinamika itt kapcsolódik össze a módszertannal: ha a hozzáférés kiépítése és aktiválása időben elválik, akkor **a fenyegetettségi szint hirtelen megugorhat anélkül, hogy új behatolás történne** – pusztán a meglévő, korábban kiépített hozzáférések aktiválásával. A hazai védelmi tervezésnek ezért nem elég a jelen pillanat nyugalmára építenie; számolnia kell azzal, hogy a látható incidensmentesség nem azonos a rendszerek érintetlenségével.

Fejlődő technológiák és a változó támadási felület

A magyar energiarendszer az elkövetkező évtizedben mélyebb technológiai átalakuláson megy keresztül, mint az előző néhány évtizedben összesen. A termelés decentralizálódása, a fogyasztásmérés digitalizálása, az energiatárolás megjelenése és a mesterséges intelligencia térnyerése együttesen olyan új eszközrétegeket visznek a rendszerbe, amelyek biztonsági szempontból még kevéssé érettek. E változó felület értékelésekor tudatosan el kell különíteni a dokumentált tényeket a következtetésektől és az előretekintő értékeléstől. Ez az elkülönítés itt különösen indokolt: a terület fiatal, a nyilvánosan dokumentált, energetikai célú incidensek száma alacsony, ezért a fenyegetettségi kép jelentős része szükségszerűen a nemzetközi trendekből és a technológia sajátosságaiból levezetett előrejelzés. A hangsúly ennek megfelelően nem az eseményeken, hanem a strukturális kockázatokon van.

A decentralizált termelés és az elosztott peremréteg

A naperőművi kapacitás gyors növekedése nem egyszerűen bővíti, hanem jellegében változtatja meg a támadási felületet. A háztartási méretű kiserőművek és a közepes ipari naperőművek százezres nagyságrendű állománya olyan eszközök tömegét viszi a rendszerbe, amelyek távoli felügyeletet és vezérlést tesznek lehetővé, jellemzően internetkapcsolaton keresztül, gyártói felhőplatformokra támaszkodva. Ezek az inverterek és vezérlőik nem a kritikus infrastruktúra hagyományos védelmi keretei között, hanem fogyasztói szintű biztonsági környezetben üzemelnek, miközben **aggregált teljesítményük rendszerszinten relevánssá vált**.

A strukturális kockázat **nem az egyedi eszközben, hanem az aggregációban rejlik**. Egyetlen kompromittált háztartási inverter a rendszer szempontjából jelentéktelen; egy gyártói vezérlőplatformon keresztül egyszerre befolyásolható eszközök nagy tömege azonban már a rendszeregyensúlyt érintő tényező. A jelenlegi nyilvános CTI-információk alapján a magyar naperőművi állomány elleni célzott, rendszerszintű manipuláció nem dokumentált; a nemzetközi szakmai elemzésekben ugyanakkor a nagy elosztottságú inverterflották koncentrált, felhőplatformon keresztüli vezérelhetősége visszatérő aggodalomként jelenik meg, és több európai elemzés mutatott ki súlyos sérülékenységeket elterjedt invertertermékekben. Szakmai következtetésként megfogalmazható, hogy a kockázat súlypontja az egyedi eszközről a gyártói vezérlőplatformra helyeződik: a támadó számára nem az egyes inverterek, hanem az őket összefogó, kevés kézben összpontosuló felügyeleti infrastruktúra jelenti az értékes célpontot. Ez a megfigyelés a decentralizáció paradox biztonsági következményét világítja meg – **a fizikailag szétaprózott termelés vezérlése logikailag újra koncentrálódik**.

E strukturális kockázatnak létezik egy jól dokumentált, valós előképe is. 2022. február 24-én, az orosz invázió napján a Viasat KA-SAT műholdas hálózatának modemjeit az AcidRain nevű törlő (wiper) kártevővel tették működésképtelenné; a támadás továbbgyűrűző hatásaként Németországban mintegy 5800 szélturbina – nagyjából 11 GW kapacitás – veszítette el a távfelügyeleti kapcsolatát. A turbinák maguk termeltek tovább, de elszakadtak a központi felügyelettől: az érintett szereplőt nem az egyes eszközökön, hanem **a közös vezérlési rétegen** keresztül érte a hatás, tömeges, határon átnyúló kiterjedéssel. A műveletet az EU és szövetségesei hivatalosan az orosz katonai hírszerzésnek tulajdonították, külön megnevezve a közép-európai szélerőműveket ért járulékos hatást. Az eset

megmutatja, hogy a megújuló termelés platformkoncentrációjából eredő rendszerszintű kockázat nem pusztán elméleti – egyetlen közös réteg kiesése egyszerre sok, fizikailag szétszórt egységet szakíthat el a felügyelettől.

Okosmérés, energiatárolás és az új adatinfrastruktúra

A fogyasztásmérés digitalizálása, az okosmérők fokozatos elterjedése és a hozzájuk kapcsolódó adatgyűjtő és -feldolgozó rendszerek új, kétirányú adatinfrastruktúrát hoznak létre a rendszerüzemeltető és a fogyasztó között. Ez az infrastruktúra üzemeltetési és piaci előnyöket kínál, biztonsági szempontból azonban két új felületet nyit meg. Az egyik a mérési adatok integritása és bizalmassága: a nagy felbontású fogyasztási adat egyszerre üzleti érték és a fogyasztói magatartás feltérképezésére alkalmas információ. A másik – és rendszerszinten súlyosabb – felület a mérőkhöz kapcsolódó vezérlési funkció, amennyiben a mérőinfrastruktúra távoli ki- és bekapcsolási vagy terheléskorlátozási képességet is hordoz; ekkor a mérőhálózat **nem csupán adatgyűjtő, hanem beavatkozó rendszerré válik**, amelynek tömeges manipulációja közvetlen rendszerhatással járhat.
Az energiatárolás terjedése hasonló logikát követ. A hálózati léptékű akkumulátoros tárolók és a fogyasztói oldali tárolórendszerek vezérléstechnikája a naperőművi inverterekhez hasonlóan hálózatba kapcsolt, távolról felügyelt és gyakran gyártói platformra támaszkodó. A tárolók sajátossága, hogy **gyors, kétirányú teljesítményszabályozásra képesek**, ami a rendszeregyensúly szempontjából értékes rugalmasság, támadói szempontból azonban pontosan azt a tulajdonságot adja, amely hirtelen, nagy amplitúdójú beavatkozásra teszi alkalmassá az eszközt. A jelenlegi nyilvános információk alapján magyar tárolórendszereket érintő biztonsági incidens nem ismert; a technológia fejlődésével és a tárolókapacitás bővülésével azonban ezek a rendszerek rendszerszintű jelentősége – és ezzel célértéke – előretekintő értékelés szerint növekszik. A közös nevező mindhárom új eszközrétegnél ugyanaz: a rendszerhatás képessége korábban a nagy, jól védett központi létesítményekhez kötődött, most pedig **a peremen, gyengébben felügyelt eszközök tömegében jelenik meg**.

A mesterséges intelligencia kettős szerepe

A mesterséges intelligencia energetikai biztonsági hatása kettős, és a két oldal jelenleg eltérő érettségi szinten áll. Védelmi oldalon az MI már ma is kézzelfogható értéket teremt: a hazai OT-védelem kulcsképességének számító anomáliadetektálás éppen az a terület, ahol a gépi tanuláson alapuló megoldások a nagy mennyiségű üzemviteli és hálózati adatból képesek kiszűrni a legitim rendszerhasználattól nehezen megkülönböztethető, gyanús viselkedést. Ez a képesség közvetlen választ ad a „living off the land" technikák jelentette detekciós kihívásra, ezért a védelmi célú MI-alkalmazás a hazai üzemeltetők számára **nem jövőbeli lehetőség, hanem a jelenben építendő kompetencia**.

Támadói oldalon a kép árnyaltabb, és itt különösen fontos a túlbecslés elkerülése. Az MI rövid távon nem új támadási képességeket teremt, hanem **a meglévőket teszi hatékonyabbá és skálázhatóbbá**: a meggyőzőbb, célzottabb adathalász üzenetek előállítását, a felderítés és a sérülékenységkeresés gyorsítását, valamint a támadói munkafolyamatok automatizálását. Ezek fokozatos, mennyiségi hatások, nem minőségi ugrások – az energetikai OT-környezet elleni, autonóm MI-vezérelt támadás jelenleg nem dokumentált, és a technológia jelenlegi állása alapján nem is a közeljövő realitása. Előretekintő értékelésként ugyanakkor megfogalmazható, hogy az MI a támadó és a védekező közötti versenyben a lépték és a sebesség dimenzióját erősíti, ami közvetve azt a szereplőt segíti, amelyik gyorsabban és nagyobb léptékben képes adaptálni – jelen helyzetben ez inkább a megfelelő erőforrásokkal rendelkező védekező, mint az opportunista támadó előnye lehet, feltéve, hogy a képesség kiépítése megtörténik.

A fejlődő technológiák nem egyszerűen új sérülékenységeket adnak a rendszerhez, hanem áthelyezik a biztonsági egyensúly súlypontjait: a védelemtől a detekció felé, a központi létesítményektől a peremréteg felé, és az egyszeri incidenskezeléstől a folyamatos, adaptív képességfenntartás felé. Ez az elmozdulás nem kezelhető pusztán technológiai beruházással; szabályozási és intézményi keretet igényel, amely biztosítja, hogy a védelmi képesség a szektor egészében, ne csak a legfelkészültebb szereplőknél épüljön ki.

Szabályozási és intézményi környezet

A fenyegetettség értékelése nem teljes annak a védelmi keretnek az ismerete nélkül, amelyben az érintett szervezetek működnek. A szabályozás és az intézményrendszer határozza meg, hogy a korábbi fejezetekben elemzett kockázatokkal a szektor egésze milyen minimumszinten képes szembenézni, és hogy hol maradnak a keretből fakadó strukturális rések. A legfőbb kérdés az, hogy a jelenlegi keret mely fenyegetésekre ad érdemi választ, és melyekkel szemben marad a védelmi képesség a szabályozáson túli tényezők függvénye. A magyar helyzet sajátossága, hogy a szabályozási keret az elmúlt években jelentősen megerősödött az európai jogharmonizáció nyomán, miközben a keret tényleges hatása a szektor rétegzett érettségi képén dől el.

A megerősödött európai és hazai keret

A hazai szabályozás gerincét az uniós NIS2 irányelv átültetése adja, amely a kiberbiztonsági alany-kört jelentősen kibővítette, és a korábbi, önkéntességre és általános elvárásokra épülő rendszert **kockázatarányos, kikényszeríthető kötelezettségekké alakította**. Az energiaszektor az irányelv logikájában **a legmagasabb kritikussági kategóriába tartozik**, ami szigorúbb felügyeleti és eseménybejelentési kötelezettséget jelent. A hazai átültetés a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben és a kapcsolódó végrehajtási rendeletekben öltött testet, a kiberbiztonsági felügyeleti feladatokat pedig – az érintett szervezeti körtől függően – a kijelölt kiberbiztonsági hatóságok, míg az incidenskezelési feladatokat a törvényben meghatározott incidenskezelő szervezetek látják el. Ez az intézményi felállás a korábbinál egyértelműbb felelősségi rendet és erősebb hatósági eszköztárat teremtett.

A keret érdemi előrelépést jelent több, korábban azonosított kockázat kezelésében. A kötelező eseménybejelentés a nyilvánosságra kerülés hiányából fakadó, a hazai fenyegetettségi képet torzító vakfoltot legalább a hatóság irányában csökkenti, javítva a szektorszintű helyzetismeretet. A kockázatarányos megközelítés elvben lehetővé teszi, hogy a védelmi elvárás a szervezet tényleges kritikusságához igazodjon, ami a rétegzett szektorban indokolt differenciálást tesz lehetővé. A vezetői felelősség kifejezett rögzítése pedig **a kiberbiztonságot a technikai szintről a szervezetirányítás szintjére emeli**.

A keret és a fenyegetettségi kép közötti eltérések

A megerősödött keret ugyanakkor nem minden kockázatra ad egyforma erősségű választ. A szabályozás természeténél fogva megfelelési kötelezettségeket ír elő, a fenyegetés viszont a megfelelési logikán túli területeken fejlődik a leggyorsabban. A living off the land technikák és az előpozicionálás elleni védelem például nem elsősorban kontrollok meglétén, hanem folyamatos észlelési és reagálási képességen múlik, amelynek minőségét a megfelelési ellenőrzés csak korlátozottan méri. Fennáll tehát annak a kockázata, hogy **a formális megfelelés és a tényleges védelmi képesség között rés nyílik** – egy szervezet lehet szabályozásilag megfelelő úgy is, hogy a legfejlettebb fenyegetések ellen érdemi észlelési képessége nincs.

A második, súlyosabb rés a szektor rétegzettségéből fakad. A magyar energiaszektor érettségi szintek szerint erősen tagolt: a nagy üzemeltetők és a távhő- vagy beszállítói réteg védelmi kapacitása között jelentős a különbség. A szabályozás kiterjesztése formálisan az utóbbi szereplőket is bevonja, **a megfeleléshez szükséges szakértelem és erőforrás azonban éppen ott szűkös, ahol a leginkább hiányzik**. A kockázatarányosság elve enyhítheti ezt a feszültséget, de nem oldja fel: egy önkormányzati tulajdonú távhőszolgáltató vagy egy kisebb integrátor számára a kötelezettségek teljesítése aránytalanul nagyobb terhet jelent, mint egy nagy energetikai társaság számára, miközben éppen ezek a legkisebb ellenállású belépési pontok. **A szabályozás önmagában nem termel szakértelmet**; ha a keret bővülését nem kíséri célzott képességtámogatás a gyengébb rétegek felé, a leggyakrabban célzott szereplők maradnak a legkevésbé védettek.

A harmadik rés a keret hatókörén kívüli függőségekhez kapcsolódik. A regionális összekapcsoltság és a néhány globális technológiai szállítótól való korrelált függés a hazai szereplők közvetlen ráhatásán kívül eső kockázat. A nemzeti szabályozás e területen természeténél fogva korlátozott: sem a szomszédos rendszerirányítók biztonsági szintjét, sem a nemzetközi technológiai platformok sérülékenységét nem képes közvetlenül befolyásolni. Ezekre a kockázatokra a válasz nem szabályozási, hanem együttműködési – az uniós és regionális információmegosztási mechanizmusokban, a közös helyzetismeret építésében rejlik, amelynek intézményi keretei léteznek, tényleges kihasználtságuk azonban a részt vevő szervezetek aktivitásán múlik. E együttműködési válasznak már ma is van hazai, kifejezetten a villamosenergia-szektorra szabott példája: a SeConSys szakmai együttműködés, amelyben a villamosenergia-ipari és a kiberbiztonsági szakemberek – szabályozási és technológiai munkacsoportokban, egyetemi és szakmai szervezetek mentorálásával –

közösen dolgoznak ki ágazati jó gyakorlatokat, és amely működési mintájául az európai energetikai információmegosztó közösség, az EE-ISAC kereteit tekinti. Az ilyen ágazati együttműködés értéke éppen abban áll, hogy a szabályozás által közvetlenül nem lefedhető területeken – a bizalmi információmegosztásban és a közös helyzetismeret építésében – teremt kapacitást.

A szakemberhiány mint keresztmetszeti korlát

A szabályozási és technológiai keret hatékonyságát végső soron egyetlen, minden területen visszatérő tényező szabja meg: az emberi kapacitás. Az OT-biztonsági és irányítástechnikai szaktudás szűkössége nem egy a kockázatok között, hanem az a keresztmetszeti korlát, amely a többi kockázatra adható válasz felső határát meghatározza. A szakemberhiány nemcsak a belső fenyegetés kockázatát növeli, hanem a védelmi képesség kiépítésének is korlátja. Az anomáliaalapú detektálás, a folyamatos hozzáférés-felderítés és az MI-alapú védelmi eszközök – tehát pontosan azok a képességek, amelyeket a fenyegetettségi kép fejlődése előtérbe helyez – mind olyan szakértelmet igényelnek, amely a hazai munkaerőpiacon a legszűkösebb.

E korlát hatása aszimmetrikus. A nagy üzemeltetők versenyképes feltételekkel meg tudják tartani a szűkös szaktudást, a gyengébb rétegek viszont nem – így **a szakemberhiány éppen azt az egyenlőtlenséget mélyíti, amelyet a szabályozás enyhíteni hivatott**. A képzési kapacitás bővítése hosszú átfutású folyamat, amely a jelenlegi fenyegetettségi szinten nem ad rövid távú választ; a reálisan járható út ezért részben **a képességek megosztásában és központi szolgáltatásként való elérhetővé tételében** keresendő, amely a szűkös szaktudást a leginkább rászoruló szereplők számára is hozzáférhetővé teszi.

Ennek a megosztott képességmodellnek szintén léteznek már hazai elemei: a nemzeti incidenskezelő szervezet olyan központi szolgáltatásokat kínál az üzemeltetők számára, amelyek egyedi kiépítése a gyengébb rétegek erőforrásait meghaladná – ilyen a gyanús állományok automatizált elemzését végző káros kód elemző rendszer, az internet felől elérhető végpontok folyamatos, központi sérülékenységvizsgálata, a célzott fenyegetettségi (CTI) tájékoztatás, valamint a döntéshozatali és kommunikációs folyamatokat gyakoroltató, szektorspecifikus gyakorlatok. E szolgáltatások logikája pontosan az, amit a fenyegetettségi kép megkíván: a szűkös szaktudást nem minden szervezetnél külön, hanem központilag, megosztott módon teszik elérhetővé, így a leginkább rászoruló – és egyben

leggyakrabban célzott – szereplők is hozzáférnek olyan képességekhez, amelyeket önállóan nem tudnának fenntartani.

Következtetések és ajánlások

A magyar energiaszektor fenyegetettségi képe jól körülhatárolható döntéshozói következtetésekbe és a belőlük közvetlenül adódó ajánlásokba sűríthető. A cél nem az általános kiberbiztonsági jó gyakorlatok megismétlése – ezeket a szabványok és a keretrendszerek részletesen tartalmazzák –, hanem azoknak a prioritásoknak a kijelölése, amelyek kifejezetten a magyar szektor sajátosságaiból következnek. Az ajánlások ennek megfelelően nem kontrollistaként, hanem döntési logikaként épülnek fel: azt jelölik ki, hová érdemes a szűkös figyelmet és erőforrást összpontosítani.

A helyzetkép fő következtetései

Az elemzés első átfogó következtetése, hogy a magyar szektor kockázati profilját **nem a legfejlettebb fenyegetés, hanem a legkevésbé védett réteg határozza meg**. A fenyegető szereplők – az opportunista kiberbűnözéstől a peremréteget célzó hacktivizmusig – következetesen **a legkisebb ellenállás irányát keresik**, a szektor pedig **érettségi szintek szerint erősen rétegzett**. A rendszerszintű kockázat ezért nem a nagy, jól védett üzemeltetőknél, hanem a távhőszolgáltatói és beszállítói rétegben, valamint a decentralizált termelés gyengén felügyelt peremén koncentrálódik. Ezt a rétegzettséget a szektor két végpontja élesen kirajzolja: a nukleáris kapacitás a hatóságilag kikényszerített, tervezési szintű védelem révén a legerősebb, míg a peremréteg a legvédtelenebb elem. Ez a felismerés **a védelmi figyelem súlypontját a leglátványosabb célpontokról a legsebezhetőbb pontok felé fordítja**.

A második következtetés, hogy a fenyegetés természete **a láthatóból a látenssé tolódik**. Az előpozicionálás és a rendszer saját eszközeit használó módszerek térnyerése azt jelenti, hogy a súlyos fenyegetés jelenléte gyakran nem jár azonnal észlelhető incidenssel; a látható incidensmentesség nem azonos a rendszerek érintetlenségével. Ez a felismerés a védelmi paradigma eltolódását követeli meg a megelőzésről és az eseménykezelésről a folyamatos észlelés és a hozzáférés-felderítés felé – olyan képesség felé, amelyet a jelenlegi megfelelési logika csak részben mér.

A harmadik következtetés, hogy a fenyegetettségi szint nem állandó, hanem **a geopolitikai környezettel együtt mozog**. A korábban kiépített hozzáférések eszkalációs időszakban aktiválódhatnak anélkül, hogy új

behatolás történne, ezért a védelmi képességet nem a nyugalmi időszak fenyegetettségéhez, hanem **a feltételezhető csúcsterheléshez kell méretezni**.
A negyedik, valamennyi korábbin átívelő következtetés pedig az, hogy a védelmi képesség felső határát **a szűkös emberi szaktudás szabja meg**, amelynek egyenlőtlen eloszlása éppen a leginkább veszélyeztetett rétegeket hagyja a legkevésbé felkészülten.

A helyzetképből következő prioritások

Az e következtetésekből adódó prioritások döntési sorrendbe rendezhetők. A magyar szektor sajátosságai alapján a legmagasabb prioritás **a védelmi képesség kiegyenlítése a szektor rétegei között**. Mivel a rendszerszintű kockázatot a leggyengébb réteg hordozza, a legnagyobb határhaszon nem a legfejlettebb szereplők további megerősítésénél, hanem a távhőszolgáltatói, kisebb beszállítói és decentralizált termelői réteg alapszintű védelmi képességének emelésénél keletkezik. Ennek reális útja – tekintettel a szakemberhiányra – nem a kötelezettségek egyszerű kiterjesztése, hanem a védelmi képességek megosztott, központi szolgáltatásként való elérhetővé tétele: közös észlelési, incidenskezelési és fenyegetettségi tájékoztató kapacitás, amely a szűkös szaktudást a leginkább rászoruló szereplők számára is hozzáférhetővé teszi.
A második prioritás **a detekciós képesség előtérbe helyezése** a megelőzés-központú szemlélettel szemben. Mivel a legfejlettebb fenyegetések a rendszer legitim eszközeit használják és időben elválasztják a hozzáférést a hatástól, a védelem súlypontját az OT-környezet viselkedésének folyamatos megfigyelésére, az anomáliaalapú észlelésre és a már meglévő, rejtett hozzáférések aktív felderítésére kell helyezni. Ez nem a megelőző kontrollok elhagyását jelenti, hanem annak felismerését, hogy egy elszánt szereplővel szemben a kérdés **nem a behatolás megakadályozása, hanem annak minél korábbi észlelése és a hatás korlátozása**.
A harmadik prioritás a bizalmi kapcsolatok – a beszállítói, karbantartói és távoli hozzáférések – **tényleges felügyelet alá vonása**. Ez a vektor a hazai szektorban egyszerre jelentős és alulkezelt: a legitim hozzáférés megkerüli a peremvédelmet, a felette gyakorolt kontroll pedig a célszervezeten kívülre esik. A prioritás gyakorlati tartalma a bizalmi hozzáférések leltározása, a jogosultságok idő- és feladatkorláthoz kötése, valamint e csatornák használatának olyan szintű megfigyelése, amely a legitim és a visszaélésszerű használat megkülönböztetését lehetővé teszi. Ide tartozik a beszállítói szoftverek és a rajtuk keresztül érkező frissítések integritásának

ellenőrzése is, mivel a legitim frissítési csatorna önmagában nem garancia a megbízhatóságra.

A negyedik prioritás **a decentralizált termelés vezérlési rétegének rendszerszintű kockázatként való kezelése**: mivel a fizikailag szétaprózott eszközök vezérlése néhány gyártói platformra fut össze, e platformok biztonsági követelményeit és a rajtuk keresztül gyakorolható aggregált beavatkozás korlátait a rendszerbiztonsági tervezés részévé kell tenni, nem pedig fogyasztói szintű kérdésként kezelni.

Az ötödik, a többit lehetővé tevő prioritás **az emberi képesség tudatos fejlesztése és megosztása**. Mivel a szaktudás szűkössége a védelmi képesség keresztmetszeti korlátja, e korlát oldása nélkül a technológiai és szabályozási előrelépés hatása is korlátozott marad. A reálisan járható út a képzési kapacitás hosszú távú bővítése mellett a meglévő szaktudás megosztásának intézményesítése – a szektorszintű együttműködés, a közös gyakorlatok és a fenyegetettségi információk aktív cseréje –, amely a rendelkezésre álló szakértelemből a lehető legnagyobb védelmi értéket termeli ki. Az ágazati együttműködésnek szintén van már hazai kerete, amelyre e prioritás építhet. Ezek a prioritások együtt nem a fenyegetés megszüntetését ígérik, ami nem reális cél, hanem a magyar szektor ellenállóképességének olyan növelését, amely a fenyegetettségi kép fejlődési irányához igazodik.

Felhasznált irodalom

ENISA. (2025) *Threat Landscape 2025.* https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf (Letöltve: 2026. augusztus. 4.)

SektorCERT. (2023) *The attack against Danish, critical infrastructure.* https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf (Letöltve: 2026. augusztus. 5.)

ENTSO-E. (2024) *First Network Code on Cybersecurity for the electricity sector has been published.* https://www.entsoe.eu/news/2024/05/24/first-network-code-on-cybersecurity-for-the-electricity-sector-published-today/ (Letöltve: 2026. augusztus. 6.)

Idaho National Laboratory (CyOTE Program). (2023) *Case Study: Davis-Besse SQL Slammer.* https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Davis-Besse-SQL-Slammer.pdf (Letöltve: 2026. augusztus. 7.)

Energy Policy (Elsevier). (2026) *Cyber threats and energy security: Development and analysis of an incident dataset for the period 2022–2024.* https://www.sciencedirect.com/science/article/pii/S0301421525004203 (Letöltve: 2026. augusztus. 7.)

Dragos. (2024) *Intel. Brief: Impact of FrostyGoop ICS Malware on Connected OT Systems.* https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology (Letöltve: 2026. augusztus. 5.)

Center for Security Studies (ETH Zürich). (2017) *Hotspot Analysis: Stuxnet.* https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf (Letöltve: 2026. augusztus. 6.)

Power Magazine (T. Sorley et al.). (2013) *What You Need to Know (and Don't) About the AURORA Vulnerability.* https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/ (Letöltve: 2026. augusztus. 7.)

E-ISAC – SANS Institute. (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case.* https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (Letöltve: 2026. augusztus. 7.)

ESET Research. (2017) *Win32/Industroyer: A new threat for industrial control systems.* https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf (Letöltve: 2026. augusztus. 5.)

Joe Slowik (Dragos, Inc.). (2019) *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.* https://pylos.co/wp-content/uploads/2022/10/VB2018-Slowik.pdf (Letöltve: 2026. augusztus. 7.)

Mandiant – Google Threat Intelligence. (2024) *APT44: Unearthing Sandworm.* https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf (Letöltve: 2026. augusztus. 5.)

ESET Research. (2017) *Industroyer: Biggest threat to industrial control systems since Stuxnet.* https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (Letöltve: 2026. augusztus. 4.)

ESET Research. (2022) *Industroyer2: Industroyer reloaded.* https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (Letöltve: 2026. augusztus. 6.)

CERT-UA. (2022) Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER. https://cert.gov.ua/article/39518 (Letöltve: 2026. augusztus. 7.)

CISA. (2020) *AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (SolarWinds Orion / SUNBURST).* https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a (Letöltve: 2026. augusztus. 7.)

CISA. (2018) *Alert TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors (Letöltve: 2026. augusztus. 6.)

CISA. (2023) *AA23-144A: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a (Letöltve: 2026. augusztus. 4.)

U.S. Department of Energy. (2021) *Colonial Pipeline Cyber Incident.* https://www.energy.gov/ceser/colonial-pipeline-cyber-incident (Letöltve: 2026. augusztus. 7.)

Recorded Future. (2025) *Insikt Group Inside DDoSia: NoName057(16)'s Pro-Russian DDoS Campaign Infrastructure.* https://www.recordedfuture.com/research/anatomy-of-ddosia (Letöltve: 2026. augusztus. 6.)

CISA. (2024) *AA24-038A: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a (Letöltve: 2026. augusztus. 7.)

CISA. (2021) *AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a (Letöltve: 2026. augusztus. 5.)

Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet. (2020) *Zsarolóvírusok – Javasolt intézkedések.* https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/zsarolovirusok-javasolt-intezkedesek/ (Letöltve: 2026. augusztus. 4.)

CISA. (2023) *AA23-335A: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a (Letöltve: 2026. augusztus. 5.)

CISA. (2024) *Identifying and Mitigating Living off the Land Techniques.* https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques (Letöltve: 2026. augusztus. 6.)

Dragos. (2026) *2026 OT/ICS Cybersecurity Report: A Year in Review.* https://www.dragos.com/ot-cybersecurity-year-in-review (Letöltve: 2026. augusztus. 7.)

Forescout. (2025) *Research – Vedere Labs SUN:DOWN – Destabilizing the Grid via Orchestrated Exploitation of Solar Power Systems.* https://www.forescout.com/resources/sun-down-research-report/ (Letöltve: 2026. augusztus. 5.)

Európai Parlament és Tanács. (2022) *Az (EU) 2022/2555 irányelv az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv).* https://eur-lex.europa.eu/eli/dir/2022/2555/oj/hun (Letöltve: 2026. augusztus. 6.)

SeConSys – NBSZ NKI. (2023) *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*. https://seconsys.eu/wp-content/uploads/2022/03/SeConSys_online_kezikonyv_2022_FINAL_22-03-03.pdf (Letöltve: 2026. augusztus. 6.)

MITRE ATT&CK. (é. n.) *Matrix for ICS – az ipari vezérlőrendszerek elleni támadói technikák osztályozási kerete.* https://attack.mitre.org/matrices/ics/ (Letöltve: 2026. augusztus. 4.)

European Union Agency for Cybersecurity (ENISA). (2023) *Good Practices for Supply Chain Cybersecurity.* https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf (Letöltve: 2026. augusztus. 7.)

Európai Bizottság. (2024) *Az (EU) 2024/1366 felhatalmazáson alapuló rendelet a határkeresztező villamosenergia-áramlások kiberbiztonsági vonatkozásaira irányadó ágazatspecifikus szabályokat megállapító üzemi és kereskedelmi szabályzatról.* https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj (Letöltve: 2026. augusztus. 7.)

1996. évi CXVI. törvény az atomenergiáról. (1996) https://njt.jog.gov.hu/jogszabaly/1996-116-00-00 (Letöltve: 2026. augusztus 7.)

1/2022. (IV. 29.) OAH rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről. (2022) https://njt.jog.gov.hu/jogszabaly/2022-1-20-8L (Letöltve: 2026. augusztus. 7.)

418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról. (2024) https://njt.jog.gov.hu/jogszabaly/2024-418-20-22 (Letöltve: 2026. augusztus. 11.)

ENISA. (2026) *NIS360 2026.* https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf (Letöltve: 2026. augusztus. 12.)

190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről. (2011) https://njt.jog.gov.hu/jogszabaly/2011-190-20-22 (Letöltve: 2026. augusztus. 7.)

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. (2024) https://njt.jog.gov.hu/jogszabaly/2024-69-00-00 (Letöltve: 2026. augusztus. 4.)

Szabályozott Tevékenységek Felügyeleti Hatósága. (2025) *NIS2 – Megjelent a kiberbiztonsági audit eljárásrendjéről és maximalizált díjáról szóló SZTFH rendelet.* https://sztfh.hu/nis2-megjelent-a-kiberbiztonsagi-audit-eljarasrendjerol-es-maximalizalt-dijarol-szolo-sztfh-rendelet/ (Letöltve: 2026. augusztus. 12.)

Forescout. (2025) *Vedere Labs SUN:DOWN – A dark side to solar energy grids.* https://www.forescout.com/resources/sun-down-research-report/ (Letöltve: 2026. augusztus. 13.)

Forescout. (2025) *Vedere Labs Uncovers Severe Systemic Security Risks in Global Solar Power Infrastructure.* https://www.businesswire.com/news/home/20250327043178/en/Forescout-Vedere-Labs-Uncovers-Severe-Systemic-Security-Risks-in-Global-Solar-Power-Infrastructure (Letöltve: 2026. augusztus. 13.)

SecurityWeek. (2024) *Vulnerabilities Exposed Widely Used Solar Power Systems to Hacking, Disruption.* https://www.securityweek.com/vulnerabilities-exposed-widely-used-solar-power-systems-to-hacking-disruption/ (Letöltve: 2026. augusztus. 13.)

SecurityWeek. (2021) *Research Shows How Solar Energy Installations Can Be Abused by Hackers.* https://www.securityweek.com/research-shows-how-solar-energy-installations-can-be-abused-hackers/ (Letöltve: 2026. augusztus. 13.)

BleepingComputer (Sergiu Gatlan). (2024) *Lynx ransomware behind Electrica energy supplier cyberattack.* https://www.bleepingcomputer.com/news/security/lynx-ransomware-behind-electrica-energy-supplier-cyberattack/ (Letöltve: 2026. augusztus. 13.)

Bitdefender. (2024) *Labs 60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States.* https://www.bitdefender.com/en-us/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states (Letöltve: 2026. augusztus. 13.)

Dark Reading. (2024) *Solar Power Installations Worldwide Open to Cloud API Bugs.* https://www.darkreading.com/ics-ot-security/solar-power-installations-worldwide-open-to-cloud-api-bugs (Letöltve: 2026. augusztus. 13.)

Euronews. (2024) *Europe's leading solar power grid is vulnerable to hackers – this is what a cyberattack could do.* https://www.euronews.com/next/2024/08/21/europes-leading-solar-power-grid-is-vulnerable-to-hackers-this-is-what-a-cyberattack-could (Letöltve: 2026. augusztus. 13.)

BleepingComputer (Bill Toulas). (2023) *Slovenia's largest power provider HSE hit by ransomware attack.* https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/ (Letöltve: 2026. augusztus. 13.)

SentinelOne – SentinelLabs (Juan Andres Guerrero-Saade – Max van Amerongen). (2022) *AcidRain: A Modem Wiper Rains Down on Europe*. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (Letöltve: 2026. augusztus. 13.)

CyberPeace Institute. (2022) *Case Study: Viasat*. https://cyberconflicts.protect.ngo/law-and-policy/cases/viasat (Letöltve: 2026. augusztus. 13.)

National Cyber Security Centre (NCSC). (2022) *Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion*. https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion (Letöltve: 2026. augusztus. 13.)

Kérdés esetén
keressen minket
az alábbi elérhetőségeink
egyikén!

Általános kérdések esetén:
titkarsag@nki.gov.hu

Hatósági kérdések esetén:
hatosag@nki.gov.hu

Incidensbejelentéssel kapcsolatos kérdések esetén:
csirt@nki.gov.hu

A riporttal kapcsolatos kérdések esetén:
cyberthreat@nki.gov.hu

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERBIZTONSÁGI
INTÉZET