Szirbik Miklós

A KIBERBIZTONSÁGRA VONATKOZÓ NIS 2 IRÁNYELV HATÁSAI A NÉMET ÉS MAGYAR JOGBAN – FELOLDHATÓK A KIBERBIZTONSÁG ÉS A VERSENYKÉPESSÉG KÖZÖTTI ELLENTÉTEK?[1]

ABSZTRAKT

2025-re világszerte előreláthatólag 41 milliárd készülék kapcsolódik majd a dolgok internetéhez, ugyanakkor Európában és világszerte egyre gyakoribbá és kifinomultabbá válnak a kibertámadások és a kiberbűncselekmények. Az Európai Unió csak az elmúlt fél évtizedben két irányelvvel szabályozta újra a kiberbiztonságra vonatkozó követelményeket az európai gazdaság, a vállalatok és a polgárok, valamint a tagállamok és az Unió védelmében. Jelen tanulmány a 2024 októberéig átültetendő úgynevezett NIS 2 irányelv fő rendelkezéseit ismerteti, valamint annak átültetésének hatásait a német és magyar jogban, összehasonlítva a NIS 2 irányelv rendelkezéseit a korábbi uniós jogszabályi környezettel, különös tekintettel a NIS irányelvben foglaltakra. Ezenfelül a NIS 2 irányelvet kontextusba helyezzük egyéb aktuális uniós jogi aktusokkal ezen a területen, például a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról szóló (EU) 2024/2847 rendelettel (a kiberrezilienciáról szóló rendelet).

[1] A tanulmány az NMHH-val kötött EM-1/1/2022. számú együttműködési megállapodásban részletezett feladatok végrehajtása céljából készült.

DOI: https://doi.org/10.36250/01284_09 • ORCID: https://orcid.org/0000-0001-7369-9949

Kulcsszavak: európai versenyképesség, kiberbiztonság, NIS irányelv, NIS 2 irányelv, átültetés, Kibertantv., biztonsági követelmények, kiberbiztonsági események, NIS 2 irányelv értelmében vett szervezetek

THE EFFECTS OF THE NIS 2 DIRECTIVE ON CYBERSECURITY IN GERMAN AND HUNGARIAN LAW – CAN THE CONFLICTS BETWEEN CYBERSECURITY AND COMPETITIVENESS BE RESOLVED?

ABSTRACT

By 2025, there will be globally approximately 41 billion devices connected to the Internet of Things while in Europe and globally the number and quality of cyberattacks and crimes committed on this field are increasing. The European Union has adopted only in the last one and a half decades two directives to regulate the requirements of cybersecurity protecting the European economy, the enterprises and citizens as well as Member States and the EU itself. This essay introduces the main regulatory elements of the new NIS 2 directive which must be implemented by October 2024, exploring also the impacts of the directive in the German and Hungarian national legal systems. This includes also a comparison of the provisions of the NIS 2 directive with earlier EU legislative frameworks in this field, especially the NIS directive. The essay also examines the context of the NIS 2 directive with other EU legislation on this field, for example Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
Keywords: European competitiveness, cybersecurity, NIS directive, NIS 2 directive, implementation, Hungarian legislative act (Kibertantv.), cybersecurity requirements, cybersecurity incidents, entities under the scope of the NIS 2 directive

BEVEZETÉS

Az Európai Bizottság felkérése alapján Mario Draghi, az Európai Központi Bank korábbi elnöke által jegyzett, 2024 szeptemberében megjelent jelentés az Európai Unió versenyképességéről (a továbbiakban: Draghi-jelentés) számos szakterület mellett a digitalizációt és az abban rejlő lehetőségeket is részletes elemzés alá veti.[2] A jelentés a 3. fejezetében *(Digitalisation and advanced technologies)* kiemeli, hogy a digitalizáció nélkülözhetetlen eszköze az európai jóléti és szociális politikák fenntartásának, valamint az uniós karbonsemlegességi célok elérésének. Ezenfelül a jelentés előrevetítése alapján a világgazdaságban az elkövetkező tíz évben előállított értékek 70%-át digitális technológiák támasztják, így Európa további lemaradása a digitális szektorban komoly kihívások elé állíthatja a kontinenst. A kibertámadások és a kiberbűncselekmények ráadásul a világon és Európában[3] egyre gyakoribbá és kifinomultabbá válnak. Ez a tendencia a jövőben várhatóan tovább fog fokozódni, tekintettel arra, hogy 2025-re világszerte előreláthatólag 41 milliárd készülék kapcsolódik majd a dolgok internetéhez.[4]

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (a továbbiakban: NIS irányelv) 2016. júliusi hatálybalépését követően 2018. május 10-től kezdve kötelezte a tagállamokat az irányelv alapján elfogadott nemzeti jogszabályok alkalmazására. Jól szemlélteti a hálózati és információs rendszerek és szolgáltatások megbízhatóságának és biztonságának lényeges szerepét a gazdasági és társadalmi biztonság szempontjából, valamint e terület gyors fejlődését az a tény, hogy a NIS irányelv szabályainak alkalmazását követően mindössze 4 és fél évvel később új uniós szabályok rendelkeznek a kiberbiztonság alapvető kérdéseiről. Az Európai Parlament és a Tanács

2 Európai Commission 2024: 67.

3 A kiberbiztonságot és az EU, valamint számos ország, illetve szervezet stratégiáit részletesen ismerteti Kovács 2018.

4 Lásd: www.consilium.europa.eu/hu/policies/cybersecurity. A témakört részletesen ismerteti Európai Unió Tanácsa 2021.

(EU) 2022/2555 irányelve (2022. december 14.) 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 (a továbbiakban NIS 2 irányelv) rendelkezéseit a tagállamok 2024. október 17-ig kötelesek átültetni, és a vonatkozó nemzeti szabályokat alapvetően 2024. október 18-tól alkalmazni.

A NIS 2 irányelv elfogadása mellett az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (a továbbiakban: DORA rendelet) is hatályba lépett, amelyet 2025. január 17-től kell alkalmazni. Ezenfelül rendes jogalkotási eljárás keretében folyamatban van az úgynevezett kiberreziliencia rendelet *(Cyber Resilience Act)*[5] elfogadása is.[6] Ennek megfelelően számos területet érint az uniós jog által támasztott kiberbiztonsági követelményeknek való megfelelési kötelezettség a tagállamok, valamint az érintett ágazati szereplők részéről is.

Jelen tanulmány a NIS 2 irányelv átültetésével hatályba lépő változásokat, a kiberbiztonság területét érintő új szemléleteket, jogintézményeket kívánja bemutatni, valamint a magyar és német jogrendszerekben kiváltott hatásokat, esetleges jogértelmezési kérdéseket ismertetni.

AZ UNIÓS JOG

A tagállamoknak 2024. október 17-ig kell elfogadniuk és kihirdetniük azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy a NIS 2 irányelvben foglaltaknak megfeleljenek. Ezenfelül a tagállamok 2025. április 17-ig kötelesek összeállítani az alapvető és fontos szervezetek, valamint a doménnév-nyilván-

5 Európai Bizottság 2022.

6 A rendes jogalkotási eljárásban jelenleg a Tanács 1. olvasat keretében megfogalmazandó állásfoglalására vár: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/0272(COD)

tartási szolgáltatásokat nyújtó szervezetek jegyzékét, amelyeket rendszeresen, de legalább kétévente kötelesek felülvizsgálni, és adott esetben frissíteni.

A NIS 2 irányelv átültetésére vonatkozó vizsgálatok előtt szükséges röviden kitérni az azt megelőző uniós jogszabályi környezetre annak érdekében, hogy pontosan bemutathassuk azokat a változásokat, amelyeket a NIS 2 irányelv elrendel a NIS irányelvhez képest. Ezt követően tekintjük át a német, illetve magyar jogalkotást, valamint azokat a felmerülő jogértelmezési, illetve gyakorlati kérdéseket, amelyeket a két jogrendszer tekintetében tárgyal a szakirodalom.

A NIS irányelv

A NIS irányelv a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiák létrehozására, a nemzeti képességek kialakítására és az egyes tagállamok által azonosított alapvető infrastruktúrákra és szervezetekre vonatkozó szabályozási intézkedések végrehajtására kötelezte a tagállamokat, a jogalkotói szándék szerint ezáltal biztosítva a hálózati és információs rendszerek biztonságára vonatkozó nemzeti keretek kiegészítését és közelítését. A NIS irányelv ezenfelül az úgynevezett együttműködési csoport,[7] valamint a nemzeti számítógép-biztonsági eseményekre reagáló csoportok hálózata[8] létrehozásával hozzájárult az uniós szintű együttműködéshez is. A fentiekben összegzett eredmények ellenére a NIS irányelv felülvizsgálata során olyan hiányosságokat tártak fel az uniós döntéshozók, amelyek gátolták a jelenlegi és a jövőben felmerülő kiberbiztonsági kihívásokkal szembeni hatékony fellépést. A legfőbb hiányosságok közé tartozik egyebek között, hogy a szolgáltatásokat nyújtó vagy gazdaságilag jelentős tevékenységeket végző szervezetekre előírt kiberbiztonsági követelmények a NIS irányelv hatálya alatt jelentősen eltértek az egyes tagállamokban a követelmények típusa, részletességi szintje és a felügyelet módja tekintetében, ami a határon átnyúló gazdasági tevékenységek versenyképességét is érintette.[9] Ezenfelül

7 NIS irányelv 4. preambulumbekezdés.
8 NIS irányelv 32. preambulumbekezdés.
9 NIS 2 irányelv 4. preambulumbekezdés.

a NIS irányelv hatálya tekintetében is lényegesek az eltérések tagállami szinten, hiszen az irányelv hatályának lehatárolása nagyrészt a tagállamok mérlegelési jogkörében maradt. Szintén tagállami mérlegelési jogkör tárgya maradt a NIS irányelv értelmében vett úgynevezett biztonsági és eseményjelentési kötelezettségek végrehajtása, így ezen a területen is lényegesek az eltérések.

A NIS 2 irányelv és a Bizottság végrehajtási jogi aktusa

A NIS 2 irányelvnek a fentieknek megfelelően az a fő célja, hogy kiküszöbölje a tagállamok közötti lényeges eltéréseket, különösen egy összehangolt szabályozási keret működésével kapcsolatos minimumszabályok megállapításával, továbbá az egyes tagállamok felelős hatóságai közötti hatékony együttműködés mechanizmusainak meghatározásával.[10] Ezenfelül a kiberbiztonsági kötelezettségek hatálya alá tartozó ágazatok és tevékenységek listája is frissül a NIS 2 irányelv hatálya alatt, valamint olyan hatékony jogorvoslatokat és végrehajtási intézkedéseket hivatott biztosítani az új irányelv, amelyek elengedhetetlenek az általuk érintett kötelezettségek tényleges érvényesítéséhez. Egyes digitális szektorbeli szereplők tevékenységének határokon átnyúló jellegére tekintettel a NIS 2 irányelv értelmében a Bizottságnak uniós szinten össze kell hangolnia a szabályokat. A Bizottság e célból kidolgozott végrehajtási rendelete[11] hivatott elősegíteni ezt a folyamatot, illetve meghatározni, hogy mely esetekben kell egy kiberbiztonsági eseményt jelentősnek tekinteni. A rendelet tervezetére vonatkozó konzultáció 2024. július 25-én lezárult, és a rendelet 2024. október 17. napján lépett hatályba.[12]

[10] A Bizottságon belüli szakértői testületek felállításával és egyéb kérdésekkel kapcsolatban a digitalizációt érintő egyéb uniós jogalkotás keretében lásd Striho–Szegedi 2023.

[11] Ref. Ares (2024)4640447–27/06/2024; A rendelet tervezete letölthető itt: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-A-digitalis-infrastruktura-szolgaltatoinak-es-az-IKT-szolgaltatasok-kezeloinek-kiberbiztonsagi-kockazatkezelesi-es-adatszolgaltatasi-kotelezettsegei_hu

[12] Lásd: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-A-digitalis-infrastruktura-szolgaltatoinak-es-az-IKT-szolgaltatasok-kezeloinek-kiberbiztonsagi-kockazatkezelesi-es-adatszolgaltatasi-kotelezettsegei_hu

A két irányelv közötti legfőbb eltérések

Tágabb hatály

A NIS 2 irányelv lényegesen kibővíti az uniós kiberbiztonsági szabályozás hatályát. A NIS irányelv hatálya alá tartozó, kritikus jelentőségű[13] ágazatok, például energetika, közlekedés, ivóvízellátás, pénzügyi infrastruktúra[14] mellett jelentősen kibővült az érintett szolgáltatások köre, amelyeket a NIS 2 irányelv két csoportra bontva vagy „kiemelten kritikus ágazatként vagy pedig egyéb kritikus ágazatként szabályozza".[15] Az új szektorok közé tartoznak például a digitális infrastruktúrák, a közigazgatás, az űralapú szolgáltatások, kivéve a nyilvános elektronikus hírközlő hálózatok szolgáltatóit, a hulladékgazdálkodás vagy az élelmiszeripar.

A NIS 2 irányelvben foglalt kötelezettségek alkalmazásának az adott ágazatba tartozás mellett további feltételei is lehetnek. Ilyen például egy bizonyos gazdasági méret elérése egyes szolgáltatók esetében. Főszabályként az irányelvet ugyanis olyan állami vagy magánvállalatokra kell alkalmazni, amelyek a 2003/361/EK ajánlás[16] mellékletének 2. cikke értelmében vett középvállalkozásoknak minősülnek vagy meghaladják az említett cikkben a középvállalkozásokra vonatkozóan előírt küszöbértékeket, feltéve, hogy az érintett szervezet az Unión belül nyújtja szolgáltatását vagy végzi tevékenységét. A főszabálytól eltérően, meghatározott esetekben, a NIS 2 irányelv hatálya méretétől függetlenül is kiterjed egy szervezetre, amennyiben például az érintett szervezet egy tagállamban az egyetlen szolgáltató egy olyan szolgáltatás tekintetében, amely elengedhetetlen a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához, vagy valamely tagállam által annak nemzeti jogával összhangban meghatározott, központi kormányzathoz tartozó közigazgatási szerv.[17]

13 NIS irányelv 5. cikk (2) bekezdés a) pontja.
14 NIS irányelv II. melléklete.
15 NIS 2 irányelv 1. és 2. sz. mellékletek.
16 A Bizottság 2003/361/EK sz. ajánlása.
17 NIS irányelv 2. cikk (2)–(4) bekezdések.

Ennek megfelelően sokkal több vállalatcsoport, illetve szektor köteles megfelelni az újított biztonsági követelményeknek, és lényeges fejlesztéseket kell tenniük a kiberbiztonsági intézkedéseik körében.

Alapvető és fontos szervezetek

A kiberbiztonsági kockázatkezelési intézkedéseknek és jelentéstételi kötelezettségeknek való megfelelés céljából a NIS 2 irányelv hatálya alá tartozó szervezeteket két kategóriába, nevezetesen az alapvető szervezetek és a fontos szervezetek közé sorolja, ami a jogalkotói szándék szerint tükrözi annak mértékét, hogy az érintett szervezetek az ágazatuk vagy az általuk nyújtott szolgáltatások típusa szempontjából mennyire kritikusak, valamint a méretüket.[18] Fontos szervezetnek minősülnek a NIS 2 irányelv I. vagy II. mellékletben említett típusú olyan szervezetek, amelyek nem minősülnek alapvető szervezetnek a NIS 2 irányelv 3. cikk (1) bekezdése értelmében, továbbá azok a szervezetek, amelyeket a tagállamok a 2. cikk (2) bekezdésének b)–e) pontja alapján fontos szervezetként azonosítanak.[19]

Szigorúbb követelmények és súlyosabb szankciók

A NIS 2 irányelv hatálya alá eső szervezet, amennyiben jelentős eseményről szerez tudomást, haladéktalanul, és minden esetben 24 órán belül köteles benyújtani egy első bejelentést. Ezenfelül a jelentős eseményről való tudomás-

18 NIS 2 irányelv 15. preambulumbekezdése.

19 Az alapvető szervezeteket a következő csoportok mentén lehet összefoglalni: 1. a kiemelten kritikus ágazatokba tartozó azon szervezetek, amelyek meghaladják a középvállalkozásokra vonatkozóan előírt küszöbértékeket; 2. az ún. minősített bizalmi szolgáltatók és a legfelső szintű doménnév-nyilvántartók, valamint a DNS-szolgáltatók, méretüktől függetlenül; 3. a nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók, amelyek középvállalkozásoknak minősülnek; 4. bizonyos közigazgatási szervek; 5. a NIS 2 irányelv I. vagy II. mellékletében említett típusú bármely egyéb szervezet, amelyet egy tagállam alapvető szervezetekként azonosított; 6. a 2022/2557 irányelv értelmében kritikus szervezetként azonosított szervezetek; 7. amennyiben a tagállam úgy rendelkezik, azon szervezetek, amelyeket az adott tagállam 2023. január 16. előtt a 2016/1148 irányelvvel (NIS irányelv) vagy a nemzeti joggal összhangban alapvető szolgáltatásokat nyújtó szereplőként azonosított.

szerzéstől számított 72 órán belül részletes eseménybejelentést kell benyújtani, azzal a céllal, hogy az érintett szervezet frissítse az első bejelentés keretében benyújtott információkat, és közölje a jelentős esemény első értékelését, annak súlyosságát és hatását, továbbá a fertőzöttségi mutatókat, amennyiben utóbbiak rendelkezésre állnak. Legkésőbb az eseménybejelentéstől számított egy hónapon belül zárójelentést kell benyújtani.[20] Amennyiben az irányelv érelmében vett alapvető szervezet megsérti e kötelezettségét, úgy legalább 10 millió EUR közigazgatási bírsággal sújtandó. Amennyiben ez magasabb, úgy a bírság legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 2%-ának megfelelő összeg, amellyel az érintett alapvető szervezet tartozik. Az irányelv értelmében vett fontos szervezet esetében ugyanez a bírság legalább 7 millió EUR, vagy ha ez magasabb, legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 1,4%-ának megfelelő maximális összege, amellyel a fontos szervezet tartozik.[21] Fontos kiemelni, hogy amennyiben a GDPR rendelet[22] 55. vagy 56. cikkében említett felügyeleti hatóságok a GDPR rendelet 58. cikke (2) bekezdésének i) pontja alapján közigazgatási bírságot szabtak ki, az illetékes hatóságok nem szabhatnak ki a NIS 2 irányelv 34. cikke szerinti közigazgatási bírságot az e cikk (1) bekezdésében említett olyan jogsértésért, amely ugyanazon magatartásból ered, mint amely a GDPR rendelet 58. cikke (2) bekezdésének i) pontja szerinti közigazgatási bírság tárgyát képezte. Az illetékes hatóságok azonban előírhatják a NIS irányelv szerinti egyéb végrehajtási intézkedéseket.

A vállalatvezetők felelősségre vonhatósága

A NIS 2 irányelv közvetlen felelősség előírását rendeli el az érintett ágazati vállalatok vezetői terhére. A tagállamok az irányelv értelmében ugyanis kötelesek biztosítani, hogy az alapvető és fontos szervezetek vezető testületei jóváhagyják az e szervezetek által a NIS 2 irányelv 21. cikkének való megfelelés érdekében tett kiberbiztonsági kockázatkezelési intézkedéseket,

20 NIS 2 irányelv 23. cikk, illetve az irányelv 102. preambulumbekezdése.

21 NIS 2 irányelv 32. cikk.

22 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete. A GDPR rendelet tagállami szintű végrehajtásából fakadó kihívásokkal kapcsolatban lásd Ruohonen–Hjerppe 2022.

felügyeljék annak végrehajtását, és felelősségre vonhatók legyenek az említett cikknek a szervezetek általi megsértéséért. Ilyen kiberbiztonsági intézkedés lehet például a NIS 2 irányelv értelmében vett kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok kidolgozása és elfogadása, vagy alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzések szervezése.

Tagállamokat érintő kötelezettségek áttekintése

Ahogy a NIS irányelv, úgy a NIS 2 irányelv is számos kötelezettséget ró a tagállamokra az átültetésen túlmenően. A legfontosabb ilyen kötelezettségek az alábbiak.

Egy lényeges tagállami kötelezettség egy nemzeti kiberbiztonsági stratégia kialakítására irányul, és annak keretében a szakpolitikák elfogadására és összehangolására a NIS 2 irányelv 7. cikke alapján. További kötelezettség az illetékes hatóságok és egyedüli kapcsolattartó pontok létrehozása vagy kijelölése a NIS 2 irányelv 8. cikke alapján. További kötelezettségi kör a nemzeti kiberbiztonsági válságkezelési keretek kijelölése vagy létrehozása (ennek keretében például hatóságok megjelölése, nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti terv kidolgozása és elfogadása és számos egyéb intézkedés) a NIS 2 irányelv 9. cikke alapján. További tagállami kötelezettség a tárgyalt irányelv 10. cikke alapján a számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: CSIRT-, *Computer Security Incident Response Team*) létrehozása vagy kijelölése, amelyek közül tagállamonként egy CSIRT-et koordinátorként kell megjelölni a sérülékenységek összehangolt közzététele céljából az irányelv 12. cikke alapján. Ezenfelül a tagállamokat fontos kötelezettségek terhelik az irányelv hatálya alá eső uniós és nemzetközi szintű együttműködés keretében, amelyek a NIS irányelvben foglalt kereteket fejlesztik tovább, így az együttműködési csoport, a CSIRT hálózat, az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: EU-CyCLONe) létrehozása, illetve e platformokban való részvétel az irányelv 14–16. cikkei alapján.

A NIS 2 irányelv hatálya alá tartozó szervezeteket érintő kötelezettségek

A NIS 2 irányelv hatálya alá eső szervezetekre alapvetően a korábbi NIS irányelv alapján kialakított követelményrendszer, illetve kötelezettségek vonatkoznak, amelyeket az új irányelv ugyanakkor sokkal részletesebben szabályoz, így a már hatályban lévő nemzeti jogszabályok vonatkozó rendelkezései is jelentős pontosításon esnek majd át.[23] A NIS 2 irányelv értelmében[24] vett alapvető és fontos szervezetek fő kötelezettségei az alábbi területeken jelennek meg. Az érintett szervezetek kötelesek megfelelő és arányos technikai, operatív és szervezési intézkedéseket meghozni annak érdekében, hogy kezeljék azokat a kockázatokat, amelyek a működésük vagy szolgáltatásaik nyújtása során használt hálózati és információs rendszerek biztonságát fenyegetik, és megelőzzék vagy minimalizálják az eseményeknek a szolgáltatásaik igénybe vevőire és más szolgáltatásokra gyakorolt hatásait. Ezeknek az intézkedéseknek a NIS 2 irányelv 21. cikk (2) bekezdése alapján legalább 10 kötelező elemet kell lefedniük, például a kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok kidolgozása vagy átdolgozása, az eseménykezelés rendszerének kialakítása, vagy az üzletmenet-folytonosság (ide érthető például, de nem kizárólag a tartalékrendszerek kezelése, valamint katasztrófa utáni helyreállítás és válságkezelés).

[23] Már a NIS irányelv átültetése is számos jogszabályt érintett, például az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, a víziközmű-szolgáltatásról szóló 2011. évi CCIX. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, a bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelet, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet, az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet. Az érintett összes jogszabályt az alábbi szakmai blog felsorolja: Pók 2018.

[24] NIS 2 irányelv 21. cikk.

Összefoglalás

Azokat a fő új elemeket, amelyeket a NIS 2 irányelv az elődjéhez képest bevezet az európai kiberbiztonsági szabályozási keretbe, az *1. táblázatban* foglaljuk össze.

1. táblázat: A NIS irányelv és a NIS 2 irányelv összevetése

Érintett terület	NIS irányelv	NIS 2 irányelv
Hatály	Kritikus szektorok	Jelentősen bővült a szektorok köre
Biztonsági követelmények	Alapvető követelmények	Szigorúbb, részletes kiberbiztonsági kockázatkezelés
Események bejelentése	72 órán belül	Első bejelentés 24 órán belül, majd részletes beszámoló 72 órán belül
Szankciók	1 millió euróig terjedő bírság vagy az éves forgalom 2%-a	10, illetve 7 millió euróig terjedő bírság vagy az éves forgalom 2%-a, illetve 1,4%-a
Felelősség	Nem szabályozza	Vállalatmenedzsment kifejezetten felelősségre vonható
Kooperáció	Nemzeti együttműködés	EU-szintű együttműködés, EU-CyCLONe bevezetése
Sérülékenységek közzététele	Nincs kifejezetten szabályozva	Sérülékenységek összehangolt közzététele
Érintett vállalatok	Nagyvállalatok	Nagy- és középméretű vállalatok (több 50 alkalmazottnál vagy 10 millió euró forgalom)

Forrás: a szerző szerkesztése

AZ ÁTÜLTETÉS A MAGYAR ÉS NÉMET JOGBAN

A német jog

A kiberbiztonság Németországban 2011 óta országos stratégiai szinten jelen van.[25] Érdemes ezzel kapcsolatban kiemelni, hogy a német közvélemény hagyományosan érzékeny a kiberbiztonságra és az adatvédelemre, ami a politikai pártok programjaiban is tetten érhető.[26] Németországban jelenleg hozzávetőleg 30 jogszabály alkalmazását érinti egyedül szövetségi szinten a kiberbiztonság kérdése.[27]

A NIS 2 irányelv hatálybalépését megelőző német szabályozás

A NIS irányelvet Németországban egy 2017. június 29-én kihirdetett törvénnyel ültették át a tagállami jogrendbe.[28]

Ezenfelül a NIS irányelv átültetését megelőző időszakban, már 2015-ben létezett egy általános IT-biztonságot szolgáló törvény (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme,* a továbbiakban: IT-Sicherheitsgesetz), amelynek hatálybalépése a szövetségi kormány által 2011-ben kidolgozott nemzeti kiberbiztonsági stratégia *(Cyber-Sicherheitsstrategie für Deutschland)*[29] első mérföldköve volt. Szintén a 2011. évi nemzeti stratégia megvalósításának részeként fogadta el a szövetségi kormány a 2014. évi digitális agendáját *(Digitale Agenda der Bundesregierung).*[30] E keretek között dolgozták ki az IT-Sicherheitsgesetz részleteit, különös tekintettel a kritikus infrastruktúrákra (a továbbiakban: KRITIS), például a villamosenergia-

25 A német gyakorlatot összevetésben számos uniós országgal ismerteti Kovács 2018.

26 Szirbik–Bernáth 2023.

27 A szövetségi kormány törvényjavaslata a NIS 2 irányelv átültetése és az információbiztonsági intézkedések lényeges alapelveinek szabályozása céljából, Gesetzentwurf der Bundesregierung 2024: 6–7.

28 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148.

29 Bundesministerium des Innern 2011.

30 Die Bundesregierung 2014.

és vízellátás, egészségügy, pénzügy vagy távközlés.[31] E rendszerek kiesése vagy a vonatkozó ellátórendszerek tartós meghibásodása a fentiekben említett agenda kidolgozói szerint drámai következményekkel fenyegetné a német társadalom egészét, a gazdaság és az állam működését. Ennek megfelelően az IT-Sicherheitsgesetz egyik fő pillére az IT-rendszerek elérhetőségének és biztonságának fokozását biztosító törvényi szabályozás megalkotása volt, különös tekintettel a kritikus infrastruktúrákra. Ezenfelül az IT-Sicherheitsgesetz a német vállalatok, valamint a szövetségi közigazgatás IT-biztonságának fokozását szolgálta, továbbá általánosan magasabb fokú védelmet hivatott biztosítani a lakosság számára is. Az IT-Sicherheitsgesetz rendelkezéseinek betartatását az Információs Technológia biztonságáért felelős Szövetségi Hivatal (*Bundesamt für Sicherheit in der Informationstechnik,* a továbbiakban: BSI) felügyelte. A kritikus infrastruktúrák üzemeltetői, amennyiben szolgáltatásukkal főszabályként elérték vagy meghaladták az 500 ezer ember ellátását jelentő határértéket, úgy kötelesek voltak legalább kétévente felülvizsgálni az IT-rendszereik biztonságát. A BSI jogosult volt esetlegesen feltárt biztonsági kockázatok elhárítását előírni. Ezenfelül a KRITIS ágazat szolgáltatóit jelentéstételi kötelezettség terhelte a BSI felé minden lényeges rendszerzavar fellépése esetében. A telekommunikációs vállalatok ezenfelül kötelesek voltak a fogyasztóikat tájékoztatni abban az esetben, ha IT-támadást észleltek, illetve a fogyasztókat útmutatókkal voltak kötelesek támogatni a veszélyhelyzet elhárítása érdekében.

A NIS 2 irányelv átültetése

A német átültetési folyamat keretében – nem utolsósorban az összetett szabályozási terület, a vonatkozó rendelkezések számos címzettje, valamint a tartományi kompetenciákat is érintő jogalkotási eljárás okán – összesen négy előadói tervezet született, amelyeket jellemzően élénk konzultáció és heves kritikák öveztek.[32] A szövetségi kormány végül 2024. július

[31] A jelen bekezdésben közölt adatokkal kapcsolatban lásd Bundesamt für Sicherheit in der Informationstechnik 2016.

[32] Lásd sokak helyett Kipker 2024.

22. napján fogadta el törvényjavaslatát.[33] A német szövetségi parlament az őszi ülésszakban tervezte tárgyalni a törvényjavaslatot, ugyanakkor a német szakirodalom,[34] illetve a parlamenti képviselők is kételkedtek abban, hogy az átültetést szolgáló törvényt sikerül-e még határidőn belül elfogadni, különösen arra való tekintettel, hogy a tartományi kompetenciákat is érintő jogszabálytervezetet a Szövetségi Tanácsnak *(Bundesrat)* is tárgyalnia kell még. Ezenfelül az időközben lebonyolított előrehozott választások, majd az ezt követő kormányalakítási koalíciós tárgyalások okán is késlekedik a német szövetségi szintű jogalkotás.[35] Tekintettel arra, hogy a törvényjavaslat hatálybalépését követően szakmai becslések szerint 30 ezer vállalkozást érint Németországban, valamint számos közigazgatási szervet, a törvényjavaslat alakulását nagy figyelem övezi.[36] Az összesen 32 szövetségi törvény, törvénykönyv vagy rendelet módosítására irányuló törvényjavaslat mindösszesen hét fő jogalkotási súlypontot azonosított, amelyeket az alábbiak szerint foglalhatunk össze.

A törvényjavaslat legfontosabb eleme kétségtelenül a fentiekben ismertetett BSI, avagy az információs technológia biztonságáért felelős szövetségi hivatal működését szabályozó törvény[37] teljes revíziója. Már az elmúlt évek során fokozatosan átalakította a jogalkotó ezt a törvényt a BSI jogállását, eljárásait, hatásköreit szabályozó törvényből egy átfogóbb kiberbiztonsági törvénnyé, amely tendencia most a NIS 2 irányelv átültetése során kiteljesül. A szabályozás központi elemeit a fenti törvény tartalmazza, amely szabályozást számos szakterületről rendelkező törvény vagy rendelet módosítása egészít ki, például a kritikus ágazatok, illetve a NIS 2 irányelv értelmében vett fontos vagy alapvető szervezetek tekintetében. További szabályozási elem a fent említett hét súlypont keretében a NIS 2 irányelv értelmében vett szervezetek definiálása és bevezetése a német jogba, a NIS 2 irányelv 21. cikk

33 A szövetségi kormány törvényjavaslata a NIS 2 irányelv átültetése és az információbiztonsági intézkedések lényeges alapelveinek szabályozása céljából: Gesetzentwurf der Bundesregierung 2024.

34 Kipker 2024: 1491.

35 Deutscher Bundestag Drucksache 20/11633.

36 Weissmann 2024; Arfwedson et al.2024; továbbá Lessner–Mayr 2024.

37 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

(2) bekezdésében felsorolt, összesen tíz minimális kiberbiztonsági kritérium bevezetése, az eddig egylépéses eseménybejelentési rendszer a NIS 2 irányelvben foglaltak alapján 3 szintű rendszerré való átalakítása, a szövetségi közigazgatást érintő új feladatok és kötelezettségek kialakítása, valamint egy föderális szintű koordinátori feladatokat ellátó hatóság felállítása: *Chief Information Security Officers* (a továbbiakban: CISO Bund). Utóbbi tekintetében még nincs eldöntve, hogy a CISO Bund a szövetségi kormány által irányítva, annak közvetlen érdekképviseletét ellátva járjon el, vagy a kormányzattól függetlenebbre alakítandó BSI-be beolvasztva.[38]

Szakmai kritikák a tervezettel kapcsolatban

Nem meglepő, hogy mivel ez egy teljesen új szabályozás olyan területen, amely új kötelezettségeket ró a címzettekre és szankciók megállapítását is lehetővé teszi, számos részletre, jogértelmezési kérdésre kiterjedő szakmai kritika éri az adott tervezetet. A NIS 2 irányelvet átültetni hivatott német tervezetet érintő összes kérdésre jelen tanulmányban terjedelmi okokból nem tudunk kitérni, ugyanakkor néhány kiemelt területet röviden ismertetünk jelen fejezetben. Összeségében megállapítható, hogy a szakirodalom feltételezései alapján számos részletkérdést a bíróságok lesznek kénytelenek tisztázni, tekintettel arra, hogy az átültetési határidőn belül a jogalkotás keretében nem sikerült minden kérdést kielégítően tisztáznia az érintetteknek.

A vállalatvezetők NIS 2 irányelv 20. cikk (1) bekezdés értelmében vett kötelezettségeire való tekintettel nem egyértelmű a német átültetési törvényjavaslat alapján, hogy a kiberbiztonsági intézkedést csak jóváhagynia kell a vezetőségnek, vagy a vezetőség köteles-e szakmailag kidolgozni az intézkedéseket, ugyanakkor a szakirodalom jellemzően a kibervédelmi intézkedések minősége érdekében amellett érvel, hogy a vezetőség csak koordinálja a kidolgozást, és ellenjegyzéssel fogadja el az eredményt.[39] Míg a korábbi előadói tervezetek értelmében korlátozható volt a vállalatvezetők belső felelőssége, a végleges tervezet egyértelművé teszi, hogy az általános német társasági jog szabályai alapján kötelesek a keletkezett károkat meg-

[38] Brecht 2024.
[39] Kuska–Wulf 2024.

téríteni a vállalat irányába is,[40] és olyan társaságok esetében, amelyekre a törvény nem ír elő ilyen belső felelősséget, a NIS 2 irányelvet átültető törvény elrendeli annak fennállását ezekre a speciális esetekre. További gyakori kritika, hogy a jogalkotó a vállalatokra vonatkozó kötelezettségeket általában nem terjesztette ki a szövetségi szintű állami intézményekre, így az állam nem mutat jó példát és nem is szerez sok közvetlen tapasztalatot az új joganyag gyakorlati kérdéseivel kapcsolatban.[41] Szintén gyakori kritika, hogy a jogalkotó nem tette egyértelművé a NIS 2 irányelv értelmében vett partnervállalkozásokkal rendelkező vagy kapcsolt vállalkozásként működő szervezetek helyzetét. A NIS 2 irányelv értelmében ugyanis, annak elkerülése érdekében, hogy alapvető vagy fontos szervezetnek tekintsék a fenti szervezeteket olyan esetben, amikor ez aránytalan lenne, a tagállamok a 2003/361/EK ajánlás[42] melléklete 6. cikke (2) bekezdésének alkalmazásakor figyelembe vehetik a szervezetek partnereikkel vagy kapcsolt vállalkozásaikkal szembeni függetlenségének mértékét. E függetlenség gazdasági, jogi és tényleges szempontú kritériumai alapvetően minden eset külön vizsgálatát teszik szükségessé, így sokáig tart majd egy megbízható joggyakorlat kialakulása, ráadásul a német jogalkotó nem illesztette be jól e fogalmakat a szabályozás kontextusába, hiszen más rendelkezések is használják e kifejezéseket, és nem egyértelmű, hogyan viszonyulnak egymáshoz ezek a tényállások.[43]

A magyar jog és a kiberbiztonság Magyarországon

A kiberbiztonság Németországhoz hasonlóan Magyarországon is a 2010-es években jelent meg átfogóbb stratégia képében, amelynek jelen formája a NIS irányelv átültetésében teljesedett ki.[44] Jelen fejezetben a NIS 2 irányelv alapján hatályba lépő változásokat ismertetjük.

[40] Például részvénytársaságok esetében a részvénytársaságokról szóló törvénynek (Aktiengesetz) a vezető tisztséget betöltő személyek általános belső felelősségére irányuló 93. §-a alapján.

[41] Kipker 2024: 1491.

[42] A Bizottság 2003/361/EK sz. ajánlása.

[43] Lessner 2024.

[44] 1035/2012. (II. 21.) Korm. határozat. Lásd továbbá Kovács 2018: 232.

A NIS 2 irányelv átültetése

Magyarországon az átültetést szolgáló törvényjavaslat kidolgozói kifejezetten korán, a NIS 2 irányelv 2024. október 17-ei átültetési határideje előtt, már 2023. március 21-én benyújtották a vonatkozó törvényjavaslatot az Országgyűlésnek.[45] Ezt követően 2023. június 13. napján elfogadták és 2023. május 15-én kihirdették a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvényt (a továbbiakban: Kibertantv.), amely lényegében átülteti a NIS 2 irányelv rendelkezéseit.[46] Fontos kiemelni ugyanakkor, hogy a NIS 2 irányelv alkalmazási körében lényeges, a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről szóló európai parlamenti és tanácsi (EU) 2022/2557 irányelv [a továbbiakban: (EU) 2022/2557 irányelv][47] átültetése során a Kormány 2024. évi őszi törvényalkotási programja keretében ezen területen további jogszabály-módosítások születtek.[48] További szabályokat az alábbi rendeletek tartalmaznak ezen a területen. A 23/2023. (XII. 19.) SZTFH rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról, a 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében

45 Miniszterelnökség 2023.

46 Kibertantv. 32. § (2) bekezdés.

47 Az (EU) 2022/2557 irányelv szerinti kritikus szervezetként azonosított szervezeteket a NIS 2 irányelv értelmében alapvető szervezeteknek kell tekinteni, illetve a tagállamok kötelesek például a NIS 2 irányelv értelmében vett kiberbiztonsági stratégiájuk keretében biztosítani egy szakpolitikai keretet az adott tagállamon belül a NIS 2 irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságai közötti fokozott koordinációhoz. Lásd NIS 2 irányelv (30) preambulumbekezdése.

48 A Kormány 2024. évi őszi törvényalkotási programja, TÖRVF-Á/5/2024., 2024. június 6. (3. tétel): Törvényjavaslat a kritikus szervezetek ellenálló képességéről szóló törvény, valamint a közbiztonságot érintő törvények módosításáról. A tervezet tartalmazza a megalkotásra váró új törvényt, valamint azon törvénymódosításokat, amelyek indokoltak az új szabályozás kialakítása miatt: www.parlament.hu/documents/d/guest/tvalk_program_2024_osz?fbclid=IwY2xjawE49C1eHRuA2FlbQIxMAABHVMXnTcBxlKrv8SNEHIRMfQEX9gyw57Tpg9ZWWlOCX9J-TCYyi-hWfG70g_aem_s6YLjfYRozOuj_Cf7KtR6g

alkalmazandó konkrét védelmi intézkedésekről, valamint a 7/2024 (VI. 24.) SZTFH rendelet a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről. A Kibertantv. alkalmazási köre nagyságrendileg 2500 vállalkozást érint Magyarországon.[49] A jogalkotó felügyeleti jogkörrel ruházta fel a Szabályozott Tevékenységek Felügyeleti Hatóságát[50] a NIS 2 irányelv hatálya alá tartozó azon vállalatok, szervezetek vonatkozásában, amelyek a társadalom és a gazdaság működése szempontjából alapvető szolgáltatásokat nyújtanak, illetve a digitalizáció fejlődése miatt nélkülözhetetlen infrastrukturális szolgáltatásokat biztosítanak. A Kibertantv. ezenfelül meghatározza a nemzeti kiberbiztonsági tanúsítási rendszerek követelményeit, a nemzeti kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjeit, valamint a törvény hatálya alá tartozó szervezeteket, illetve definiálja az alapfogalmakat.

Szakmai kritikák a hazai szabályozással kapcsolatban

Németországhoz hasonlóan Magyarországon is megfigyelhető az új fogalmak és jogintézmények alkalmazására vonatkozó bizonytalanság, illetve a szakmai szereplők és szakjogászok kritikája a jogalkotó által elkövetett vélt vagy valós mulasztások, nem egyértelmű fogalommeghatározások tekintetében. Egy ilyen kritika például arra vonatkozik, hogy nem ültették át pontosan a NIS 2 irányelv azon rendelkezését, miszerint a hatálya alá tartozó szervezeteket a letelepedésük szerinti tagállam joghatósága alá tartozónak kell tekinteni. A nyilvános elektronikus hírközlő hálózatok szolgáltatóit vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókat azonban azon tagállam joghatósága alá tartozónak kell tekinteni, ahol szolgáltatásaikat nyújtják, és a Kibertantv. ezt a kivételt a kritikák alapján nem szabályozza.[51]

[49] Hetényi–Menczelesz 2024.

[50] Szabályozott Tevékenységek Felügyeleti Hatósága: https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitas/kiberbiztonsagi-felugyelet/

[51] Kozma–Almásy 2024.

ÖSSZEGZÉS

Mindkét vizsgált ország átfogó revízió alá vetette a kiberbiztonságra vonatkozó nemzeti jogszabályait. A NIS 2 irányelv új jogintézményei, részletesebb kiberbiztonsági követelményei, jóval tágabb címzettek köre és tárgyi hatálya okán számos részletkérdésben számíthatunk arra, hogy jogértelmezési bizonytalanság jellemzi majd a nemzeti jogszabályok hatálybalépését követő időszakot, így a nemzeti bíróságoknak és az előzetes döntéshozatali eljárás keretében az Európai Unió Bíróságának, valamint az Európai Bizottságnak fontos szerepe lesz e kérdések tisztázásában. Ezenfelül a tagállamokban már a NIS 1 irányelv hatálya alatt kialakuló piaci szereplők kiberbiztonsági tanácsadásra irányuló szolgáltatásai is nagymértékben segíthetik a kiberbiztonság szempontú gyakorlatok egységes szabványok szerinti kialakulását az adott nemzeti stratégiákkal és előírásokkal összhangban. Érdemes ugyanakkor a jelen tanulmány bevezető részében hivatkozott Draghi-jelentésre is visszautalni, amely alapján a digitális technológiák meghatározó szerepet játszanak a világgazdaság előttünk álló évtizedében, ugyanakkor az Európai Unióra jellemző túlszabályozási tendencia ezen a területen is versenyhátrányt okozhat az európai gazdasági szereplőknek.[52] A NIS 1-2 irányelvek gyors szabályozási üteme, valamint a jelen tanulmányban tárgyalt tagállamokban megfigyelhető átültetési nehézségek és adminisztratív terhek – például az egyedül Magyarországon a NIS 2 irányelv által érintett 2500 vállalkozó – jól szemléltetik, hogy Európa gazdaságának versenyképessége szempontjából mennyire létfontosságú az arányos jogalkotás.

[52] A Draghi-jelentés deregulációt, és egyszerűbb szabályozást javasol a kiberbiztonság területén is. European Commission 2024: 76.

FELHASZNÁLT IRODALOM

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Arfwedson, Jan – Döring, Andre – Dünn, Hans-Wilhelm – Harthun, Hannes – A Bizottság 2003/361/EK sz. ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg)

Az Európai Unió Tanácsa (2021): *Tervezet – A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról.* Brüsszel, 2021. március 9. Online: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/hu/pdf

Brecht, Christian (2024): Zuversicht beim CISO. *Behörden Spiegel,* 2024. július 2. Online: www.behoerden-spiegel.de/2024/07/02/dahns-zuversicht-beim-ciso/

Bundesamt für Sicherheit in der Informationstechnik (2016): *Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen.* Online: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=1

Bundesministerium des Innern (2011): *Cyber-Sicherheitsstrategie für Deutschland.* Online: https://cyber-peace.org/wp-content/uploads/2013/05/DE_cyberSecurityStrategie.pdf

Deutscher Bundestag Drucksache 20/11633, 20. Wahlperiode 04.06.2024: Antrag der Fraktion der CDU/CSU Cyberresilienz stärken und kritische Infrastrukturen wirksam schützen – NIS-2-Richtlinie unverzüglich umsetze. Online: https://dserver.bundestag.de/btd/20/116/2011633.pdf

Die Bundesregierung (2014): *Digitale Agenda 2014 – 2017.* Online: www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=1

Európai Bizottság (2022): *Javaslat Az Európai Parlament és a Tanács rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról. COM(2022) 454 final.* Online: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0003.02/DOC_1&format=PDF

European Commission (2024): *The Future of European Competitiveness, In-depth analysis and recommendations (Part B).* 2024 szeptember 9. Online: https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

Gesetzentwurf der Bundesregierung (2024): *Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz).* Online: www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamenSicherheitsniveaus von Netz- und Informationssystemen in der Union.

Gombos Katalin (2023): A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban. *In Medias Res,* 12(2), 92–119. Online: https://doi.org/10.59851/imr.12.2.5

HeténYi Kinga – Menczelesz Adrián (2024): NIS2 a kiberbiztonságért – Június 30. az első fontos határidő a cégeknek! – Mely társaságoknak milyen ütemtervet ír elő az új jogszabály és mik a szankciók meg nem felelés esetén? *Jogi Fórum,* 2024. június 25. Online: www.jogiforum.hu/hir/2024/06/25/nis2-a-kiberbiztonsagert-junius-30-az-elso-fontos-hatarido/

Kovács László (2018): *Kiberbiztonság és -stratégia.* Budapest: Dialóg Campus.

Kipker, Dennis-Kenji (2024): NIS2UmsuCG: Wie viel Neues enthält der aktuelle Referentenentwurf vom 7.5.2024? *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung,* 1488–1491.

Kozma Zoltán – Almásy Márk (2024): NIS2 irányelv: 2024. június 30. a nyilvántartásba vételi határidő az érintett szervezetek részére. *Advocatus. A DLA Piper Hungary Jogi Blogja,* 2024. június 26. Online: https://blogs.dlapiper.com/advocatus/2024/06/nis2-iranyelv-2024-junius-30-a-nyilvantartasba-veteli-hatarido-az-erintett-szervezetek-reszere/

Kuska, Michael – Wulf, Hans M. (2024): NIS2-Richtlinie: Update zum deutschen Umsetzungsgesetz und der neuen EU-Durchführungsverordnung. *Heuking,* 2024. július 2. Online: www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/nis2-richtlinie-update-zum-deutschen-umsetzungsgesetz-und-der-neuen-eu-durchfuehrungsverordnung.html

Lessner, Anne – Mayr, Lucas (2024): Besonderheiten für Konzerne in den NIS-Richtlinien und dem BSIG. *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung,* (2), 148–153.

Lessner, Anne (2024): Konzernspezifische Änderungen aus der NIS2-Richtlinie und ihre Umsetzung. *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung,* 226–231.

Löw, Alexander (2024): *Positionspapier zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG).* Berlin: Cyber-Sicherheitsrat Deutschland e.V. Online: https://cybersicherheitsrat.de/wp-content/uploads/Positionspapier-zur-NIS2-Umsetzung-des-CSRD-e.V.pdf

Miniszterelnökség (2023): *A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről.* Törvényjavaslat iromány száma: T/3314. Benyújtó: Dr. Semjén Zsolt, miniszterelnök-helyettes. Online: www.parlament.hu/irom42/03314/03314.pdf

PÓK László (2018): A GDPR árnyékában: a hálózati és információs rendszerek biztonságára vonatkozó új szabályok. *GDPR-blog,* 2018. május 14. Online: https://gdpr.blog.hu/2018/05/14/a_gdpr_arnyekaban_a_halozati_es_informacios_rendszerek_biztonsagara_vonatkozo_uj_szabalyok

RUOHONEN, Jukka – HJERPPE, Kalle (2022): The GDPR Enforcement Fines at Glance. *Information Systems,* 106. Online: https://doi.org/10.1016/j.is.2021.101876

STRIHÓ Krisztina – SZEGEDI László (2023): A digitális egységes piac kezdeti lépései. *Pro Publico Bono – Magyar Közigazgatás,* 11(4), 127–147. Online: https://doi.org/10.32575/ppb.2023.4.7

SZIRBIK, Miklós – BERNÁTH Sára (2023): A Digital Markets Act és a Digital Services Act várható hatásai a német jogrendszerben a magyar gyakorlat szempontjából. *In Medias Res,* 12(2), 169–189. Online: https://doi.org/10.59851/imr.12.2.8

WEISSMANN, Paul (2024): *NIS2 Umsetzungsgesetz.* Online: www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html