A hálózatbiztonság jogi vonatkozásai

Durczy Levente[1], Molnár András[2]

Óbudai Egyetem, Neumann János Informatikai Kar [1]durczy.levente@uni-obuda.hu, [2]molnar@uni-obuda.hu

Absztrakt: *Ebben a cikkben megvizsgálunk néhány nemzetközi-EU- és magyar hálózatbiztonsági jogi keretet, összefoglaljuk és felvázoljuk a lehetséges irányokat annak érdekében, hogy a jogszabályi szabályozás a lehető leggyorsabban alkalmazkodni tudjon az új technológiákhoz és az ebből fakadó kihívásokhoz. az egyre gyorsuló technikai fejlődés. A mai világban az adat, az informatika és a hálózatbiztonság szorosan összefonódó fogalmak, ezért a jogszabályok többnyire együtt kezelik őket, így vizsgálatunk témája is ehhez igazodik.*

Kulcsszavak: hálózatbiztonság, jogi szempontok, jogi szabályozás, kiberbiztonság,

Bevezetés

A hálózati biztonság a számítógépes hálózatok jogosulatlan hozzáféréstől, lopástól, megszakítástól vagy egyéb rosszindulatú tevékenységektől való megvédésének gyakorlatát jelenti. Különféle technológiák, folyamatok és irányelvek megvalósítását foglalja magában, amelyek megvédik a hálózatokat a fenyegetésektől, beleértve a vírusokat, rosszindulatú programokat, hackelési kísérleteket és az illetéktelen hozzáférést.

A kiberfenyegetések és támadások több csoportba sorolhatók: rosszindulatú programok, Dos-támadások, webes támadások, biztonsági rések, munkamenet-eltérítés, bennfentes fenyegetések, DNS-mérgezés. (Easttom C. 2019)

Ahogy Srinivas és Kumar (2019) leírja, a hálózati biztonsági intézkedések közé tartoznak a tűzfalak, vírusirtó szoftverek, behatolásészlelő és -megelőzési rendszerek, virtuális magánhálózatok (VPN), titkosítás és egyéb biztonsági technológiák. Ez magában foglalhatja irányelvek és eljárások bevezetését is annak biztosítására, hogy az alkalmazottak megfelelően használják a hálózati erőforrásokat, és kövessék a legjobb biztonsági gyakorlatokat (Khan, MJ 2023).

A hatékony hálózati biztonság kulcsfontosságú az érzékeny adatok védelmében, az üzletmenet folytonosságának fenntartásában és annak biztosításában, hogy a hálózati erőforrások a jogosult

felhasználók rendelkezésére álljanak. Ez egy folyamatos folyamat, amely folyamatos megfigyelést és frissítéseket igényel, hogy az új fenyegetések és sebezhetőségek előtt maradjon.(Ali, 2017), (Keszhelyi, 2015)

A hálózatok biztonsága jogi úton többféleképpen szabályozható. Az egyik megközelítés jogi keret létrehozása a hálózatok biztonságának javítására. Az ilyen keretrendszerek általában kiberbiztonsági törvények és rendeletek, amelyek biztonsági követelményeket támasztanak a vállalatok és szervezetek számára, és meghatározzák azokat a jogi követelményeket, amelyeknek a szervezeteknek meg kell felelniük.

Ezenkívül a jogi eszközök közé tartoznak a szankciók, a büntetések, valamint az azonosítás és a vizsgálat. Az ilyen típusú jogi eszközök a kiberbűnözés megelőzésére és a támadások elleni védekezés megerősítésére összpontosítanak. Az azonosítási és nyomozási módszerek hatékonyak a bűnözők azonosításában, míg a szankciók és büntetések jelentős hatással lehetnek a potenciális támadók viselkedésére és a szervezetek biztonsági gyakorlatára.

Végül a jogi eszközök közé tartoznak az együttműködési megállapodások és kötelezettségvállalások. Az ilyen típusú jogi eszközök javítják a szervezetek közötti együttműködést a kiberbiztonsági kérdésekben, és javítják a biztonsági protokollokat és követelményeket. Az együttműködési megállapodások és kötelezettségvállalások lehetővé teszik az adatvédelmi, biztonsági és jogi kérdések közös megoldását, és ezáltal hozzájárulnak a hálózatok biztonságának javításához.

Jogi szabályozási példák

Az országok kiber- és hálózatvédelmének szintje nagymértékben függ az adott ország jogi, műszaki, gazdasági és kulturális környezetétől, valamint a rendelkezésre álló erőforrásoktól és a politikai akarattól. Ezért nehéz egyértelműen meghatározni, hogy melyik ország rendelkezik a legmagasabb szintű kibervédelemmel. Vannak azonban olyan országok, amelyek nagy hangsúlyt fektetnek a kibervédelemre, és a tapasztalatok szerint ők rendelkeznek a legfejlettebb kiberbiztonsági infrastruktúrával és stratégiával. Ilyen országok például az Egyesült Államok, az Egyesült Királyság, Japán, Izrael, Németország és Svédország.

A kiberbiztonsági infrastruktúra elemei a következők:

- Hálózati eszközök: A hálózati eszközök olyan hardverek és szoftverek, amelyek lehetővé teszik a hálózati kommunikációt. Ide tartoznak az útválasztók, kapcsolók, tűzfalak, proxy-k és egyéb eszközök.

- Adatközpontok: Az adatközpontok olyan helyek, ahol a rendszereket, szervereket és adatbázisokat tárolják. A kiberbiztonsági infrastruktúra részeként az adatközpontok mind fizikai, mind logikai védelemmel vannak ellátva.
- Szerverek és rendszerek: A szerverek és rendszerek azok az eszközök, amelyek lehetővé teszik az adatok tárolását és feldolgozását. Ide tartoznak a fájl- és adatbázisszerverek, felhőszolgáltatások, virtuális környezetek és egyéb rendszerek.
- Biztonsági szoftver: A biztonsági szoftverek olyan programok, amelyek megvédik a rendszert a különféle fenyegetésektől. Ez magában foglalja a víruskereső és tűzfalprogramokat, a biztonsági incidenskezelő rendszereket, a beléptető- és azonosító rendszereket és más biztonsági szoftvereket.
- Irányelvek és folyamatok: A kiberbiztonsági infrastruktúra magában foglalja azokat az irányelveket és folyamatokat, amelyek segítenek fenntartani a biztonságot. Ez magában foglalja a biztonsági szabályzatokat, az incidenskezelési folyamatokat, a biztonsági auditokat és egyéb folyamatokat.
- Emberek: Az emberek fontos szerepet játszanak a kiberbiztonsági infrastruktúrában, amikor rendszereket kezelnek és felügyelnek. Ide tartoznak az informatikai szakemberek, a biztonsági szakemberek, az incidenskezelők és más dolgozók.

Az alábbiakban felsorolunk néhány országot, amelyek jelenleg a legfejlettebb kiber- és hálózatbiztonsági infrastruktúrával rendelkeznek:

- Izrael: Izrael a kiberbiztonsági innováció központja, a kormány évek óta komoly erőfeszítéseket tesz az ország kiberbiztonsági védelmének megerősítésére.
- Egyesült Államok: Az Egyesült Államok globális vezető szerepet tölt be a kiberbiztonság fejlesztésében, és számos kiberbiztonsági szervezetnek, intézménynek és egyetemnek ad otthont.
- Egyesült Királyság: Az Egyesült Királyság számos nagy kiberbiztonsági cégnek ad otthont, és a brit kormány is jelentős figyelmet fordít a kiberbiztonsági kérdésekre.
- Németország: Németország vezető gazdaság az Európai Unióban, és a kiberbiztonsági szakértők szerint az ország kiberbiztonsági infrastruktúrája is nagyon fejlett.
- Szingapúr: Az ázsiai régióban Szingapúr kiemelkedő szerepet játszik a kiberbiztonsági fejlesztésekben, a városállam kormánya komoly erőfeszítéseket tesz a kiberbiztonsági védelem javítására.

A kiberbiztonsággal kapcsolatos politikai és stratégiai vezetés általában a legmagasabb szintű politikai szintek hatáskörébe tartozik. Az a tény, hogy a kiberbiztonság a legmagasabb politikai szinteken található, hangsúlyozza mind a kérdés fontosságát, mind azt a tényt, hogy civil vezetés alá tartozik. A legtöbb államban a belügyminisztérium és a védelmi minisztérium is intézményesen részt vesz a kiberbiztonságban a miniszterelnöki hivatalok mellett (Baezner, Cordey 2019).

Ha a magyar kiber- és hálózati biztonság fejlettségének és jogi környezetének állapotát és színvonalát akarjuk vizsgálni, akkor a világ legfejlettebb rendszerekkel rendelkező országainak, valamint a legközelebbi miatt az Európai Unió jogi környezetét kell vizsgálnunk. gazdasági és politikai kapcsolatok. Ezen országok szabályozási környezetének ismerete fontos támpontokat adhat a magyar szabályozás fejlettségi szintjének emeléséhez, ezért a következőkben áttekintjük Izrael, az USA és az EU jogrendszerének kiberbiztonsági vonatkozásainak legfontosabb pontjait.

Izrael:

Izraelben az adatbiztonságot, a hálózatbiztonságot és az információbiztonságot különféle törvények és rendeletek szabályozzák. Az egyik legjelentősebb törvény az adatvédelmi törvény, amely a személyes adatok szervezetek általi gyűjtését, tárolását és felhasználását szabályozza. Ezenkívül az izraeli büntető törvénykönyv kriminalizálja a kiberbűnözés különféle típusait, például a hackelést, a számítógépekhez való jogosulatlan hozzáférést, valamint a rosszindulatú szoftverek létrehozását és terjesztését.

Az izraeli kormány több testületet is létrehozott az információbiztonság felügyeletére és szabályozására. Például az Israel National Cyber Directorate (INCD) felelős a nemzeti politika meghatározásáért, valamint a kibertámadások megelőzésére és az azokra való reagálásra irányuló erőfeszítések összehangolásáért (Christiano F. 2020). Az INCD együttműködik más kormányzati szervekkel, valamint a magánszektor szervezeteivel a kiberellenállóság előmozdítása és a kritikus infrastruktúra védelme érdekében.

Másképpen fogalmazva, az INCD egy olyan kormányzati ügynökség, amely az ország digitális eszközeinek és kritikus infrastruktúrájának a kiberfenyegetésekkel szembeni védelméért felelős. A Miniszterelnökség alatt működik, és 2015-ben alakult.

Az INCD feladata a nemzeti kiberpolitika kialakítása, útmutatás és segítségnyújtás a kormányzati szerveknek, kutatási és fejlesztési tevékenységek végzése, valamint a kiberbiztonság fokozására irányuló erőfeszítések összehangolása az állami és a magánszektorban. Ezenkívül előmozdítja a nemzetközi együttműködést a kiberügyekben, és képviseli Izraelt különféle kiberrel kapcsolatos fórumokon.

Céljai elérése érdekében az INCD szorosan együttműködik a különböző érdekelt felekkel, beleértve a kormányzati szerveket, a tudományos intézményeket, az iparági partnereket és a nemzetközi szervezeteket. Számos műveleti egységet is üzemeltet, például a Computer Emergency Response Team-et (CERT) és a Kiberoktatási Központot, amelyek számos szolgáltatást nyújtanak, beleértve az incidens-reagálást, a fenyegetés-felderítést és a képzést.

Összegezve kijelenthető, hogy az INCD kritikus szerepet játszik Izrael kiberterének ellenálló képességének biztosításában, és magas színvonalú tevékenysége kulcsszerepet játszik abban, hogy a világban Izraelnek globális vezető szerepe van a kiberbiztonsági technológiák alkalmazása terén.

Egy másik fontos szabályozás a kibervédelmi törvény, amely megköveteli bizonyos szervezetektől kiberbiztonsági intézkedések végrehajtását és a kiberincidensek jelentését a kormánynak. A törvény a kormányzati szervekre, a kritikus infrastruktúra-szolgáltatókra és más, érzékeny információkat kezelő szervezetekre vonatkozik.

Izrael kibervédelmi törvénye, más néven Kibertörvény, egy olyan jogszabály, amelyet a Knesszet, az izraeli parlament fogadott el 2002-ben. A törvény célja, hogy jogi keretet biztosítson az izraeli nemzetbiztonságot fenyegető számítógépes fenyegetések kezeléséhez, beleértve a az ország kritikus infrastruktúrájának védelme a kibertámadásokkal szemben. Ez a törvény keretében került megalakításra később az Izraeli Kiberbiztonsági Igazgatóságot (INCD), mint Izrael kiberbiztonsági stratégiájának felügyeletéért felelős elsődleges ügynökség, valamint az Izraeli Nemzeti Kiberbiztonsági Hatóság (INCSA).

Az INCD egy kormányzati ügynökség, amely a Miniszterelnöki Hivatal alatt működik, és felelős az ország átfogó kiberbiztonsági politikájának koordinálásáért és felügyeletéért. Középpontjában Izrael kibervédelmi képességeinek fejlesztése, a kiberincidensek és vészhelyzetek kezelése, valamint a kutatás és fejlesztés előmozdítása áll.

Az INCSA felelős az izraeli kritikus infrastruktúrák kiberbiztonságának szabályozásáért és felügyeletéért, beleértve az energiát, a pénzügyeket és a közlekedést. Irányelveket és előírásokat ad ezen infrastruktúrák védelmére, és biztosítja, hogy megfeleljenek a kiberbiztonsági szabványoknak.

A kibervédelmi törvény számos kötelezettséget ír elő a köz- és magánjogi jogalanyok számára az információs rendszerek védelmével kapcsolatban, beleértve a biztonsági események jelentésére és a biztonsági ellenőrzések végrehajtására vonatkozó követelményeket. A törvény rendelkezéseket tartalmaz a kiberbiztonsági szabványok és iránymutatások megállapítására, valamint a kormányzati szervek és a magánszervezetek közötti információmegosztásra is a kiberfenyegetésekre adott válaszok jobb összehangolása érdekében.

A Kibertörvényt a kezdeti elfogadása óta többször frissítették, legutóbb 2018-ban a kibervédelmi törvény (5. módosítás) elfogadásával. Ez a módosítás új rendelkezésekkel egészítette ki a kiberszolgáltatók szabályozását és az INCD nemzeti kiberbiztonsági incidensek kezelésében betöltött szerepének erősítését.

A kibervédelmi törvény 5. számú módosítását, más néven a számítógépes rendszerek védelméről szóló rendeletet azért léptették életbe Izraelben, hogy fokozzák az ország kiberbiztonsági védelmét. A módosítás frissítette az eredeti, 2002-es kibervédelmi törvényt, amelynek célja az volt, hogy kezelje az elmúlt években felmerült új fenyegetéseket és kihívásokat.

A módosítás kibővítette azon szervezetek körét is, amelyeknek be kell tartaniuk a kiberbiztonsági előírásokat. A kormányhivatalokon és a kritikus infrastruktúrák üzemeltetőin kívül a törvény a jogalanyok szélesebb körére terjed ki, beleértve a pénzügyi intézményeket, a közszolgáltatókat és az egészségügyi szolgáltatókat.

A kibervédelmi törvény 5. számú módosítása azt is megköveteli a szervezetektől, hogy jelentsenek minden jelentős kiberbiztonsági incidenst az INCD-nek, és előírja, hogy számos technikai és szervezeti intézkedést hajtsanak végre hálózataik és adataik védelme érdekében. Ezek az intézkedések magukban foglalják a rendszeres kockázatértékelések elvégzését, az incidensekre reagáló tervek kidolgozását, valamint az adattitkosítási és hozzáférés-ellenőrzési intézkedések végrehajtását.

A módosítás olyan rendelkezéseket is tartalmaz, amelyek ösztönzik a köz- és a magánszféra közötti fokozottabb együttműködést a kiberbiztonság területén, ideértve egy új kiberbiztonsági innovációs központ létrehozását a területen végzett kutatás és fejlesztés előmozdítása érdekében. Végül a törvény szankciók és pénzbírságok kiszabását írja elő a rendelkezéseinek be nem tartása esetén, beleértve a szervezet működésének esetleges felfüggesztését súlyos jogsértés esetén.

USA:

Az Egyesült Államokban az adatbiztonságot, a hálózatbiztonságot és az információbiztonságot számos szövetségi és állami törvény és rendelet szabályozza. A legfontosabb szövetségi törvények közül néhány:

- Az Egyesült Államok egyik legrégebbi, számítógépes biztonságot érintő jogszabálya az 1987-es Computer Security Act. Ez előírja a kormányzati szerveknek, hogy azonosítsák az érzékeny rendszereket, tartsanak számítógépes biztonsági képzést, és dolgozzanak ki számítógépes biztonsági terveket. Ez a törvény egy homályos felhatalmazás volt, amely az Egyesült Államok szövetségi szerveit utasította biztonsági intézkedések bevezetésére, de nem határoz meg semmilyen szabványt. Ez a jogszabály jogi felhatalmazást adott konkrét szabványok elfogadására, előkészítve az utat a jövőbeli iránymutatások és szabályozások számára6.
- A számítógépes csalásról és visszaélésről szóló törvény (CFAA) az Egyesült Államok törvénye, amelyet 1986-ban fogadtak el a számítógéppel kapcsolatos bűncselekmények, például a hackelés, az információ lopás és a kiberbűnözés egyéb formái kezelésére. A CFAA alapján törvénysértés a számítógéphez való szándékos, engedély nélküli vagy jogosultságot meghaladó hozzáférés, valamint az ilyen jogosulatlan hozzáférésből származó információk felhasználása vagy nyilvánosságra hozatala. Tiltja továbbá a számítógépben kárt okozó program, kód vagy parancs tudatos futtatását és továbbítását, és törvénysértések esetén büntetőjogi szankciókat ír elő.
- A CFAA az évek során többször módosult. Kiemelhető például a 2001-es Patriot Act, amelyet nem sokkal a szeptember 11-i terrortámadás után fogadtak el. Ez kiterjesztette a törvény hatályát a terrorizmussal kapcsolatos bűncselekményekre is. A CFAA bizonyos körökben ellentmondásos volt, a kritikusok azzal érvelnek, hogy túlságosan tág, és arra használták, hogy egyéneket olyan magatartások miatt vádoljanak, amelyek valójában nem károsak, például a szolgáltatási szerződések feltételeinek megsértése miatt. A törvény támogatói ugyanakkor azzal érvelnek, hogy meg kell akadályozni a kiberbűnözést, és meg kell védeni az érzékeny információkat az illetéktelen hozzáféréstől.
- Az Electronic Communications Privacy Act (ECPA): Ez a törvény szabályozza a kormányzati hozzáférést az elektronikus kommunikációhoz, például az e-mailekhez és az azonnali üzenetküldéshez.

- Az egészségbiztosítási hordozhatóságról és elszámoltathatóságról szóló törvény (HIPAA): Ez a törvény szabványokat határoz meg az egyének egészségügyi információinak védelmére, és előírja az egészségügyi szolgáltatók számára, hogy biztonsági intézkedéseket hajtsanak végre a betegek adatainak védelme érdekében.
- A Gramm-Leach-Bliley törvény (GLBA): Ez a törvény előírja a pénzügyi intézményeknek, hogy biztonsági intézkedéseket hajtsanak végre a fogyasztói adatok védelme érdekében.
- A szövetségi információbiztonság modernizációs törvénye (FISMA) az Egyesült Államok 2014-ben elfogadott szövetségi törvénye, amely előírja a szövetségi ügynökségek számára, hogy információbiztonsági programokat hajtsanak végre, hogy megvédjék információikat és információs rendszereiket a jogosulatlan hozzáféréstől, felhasználástól, nyilvánosságra hozataltól, megzavarástól, módosítástól vagy megsemmisítéstől. A FISMA azt is megköveteli a szövetségi ügynökségektől, hogy olyan kockázatkezelési folyamatokat dolgozzanak ki és tartsanak fenn, amelyek integrálják a biztonságot a szövetségi információs rendszerek életciklusába.
- A FISMA értelmében a szövetségi ügynökségeknek rendszeres időközönként értékelniük kell információbiztonsági programjaikat, hogy megállapítsák azok hatékonyságát és azonosítsák a gyengeségeket vagy hiányosságokat. Emellett kötelesek jelenteni minden jelentős biztonsági incidenst vagy sebezhetőséget a Belbiztonsági Minisztériumnak (DHS) és a Menedzsment és Költségvetési Hivatalnak (OMB). Ezenkívül a FISMA megköveteli a szövetségi ügynökségektől, hogy megfeleljenek a különböző biztonsági szabványoknak, beleértve a Szövetségi Információfeldolgozási Szabványokat (FIPS) és a Nemzeti Szabványügyi és Technológiai Intézet (NIST) irányelveit.
- A FISMA csak a szövetségi ügynökségekre vonatkozik, és nincs közvetlen hatása a magánszektor szervezeteire. Mindazonáltal befolyást gyakorolt az információbiztonsági gyakorlatok és szabványok kialakítására a szövetségi kormányon belül, és számos magánszektorbeli szervezet a FISMA-szerű biztonsági keretrendszert fogadta el legjobb gyakorlatként.
- Általános adatvédelmi rendelet (GDPR): Ez egy olyan európai uniós szabályozás, amely az EU-lakosokkal üzletelő amerikai vállalatokat érinti, és megköveteli a szervezetektől bizonyos adatvédelmi intézkedések végrehajtását.

Ezeken a szövetségi törvényeken kívül sok állam rendelkezik saját adatvédelmi incidens bejelentési rendeletekkel és jogszabályokkal, amelyek előírják a vállalatoknak, hogy értesítsék az egyéneket személyes adataik megsértése esetén. Különféle iparág-specifikus szabályozások is léteznek, mint például a Payment Card Industry Data Security Standard (PCI DSS) a hitelkártyaadatokat kezelő szervezetek számára.

Összességében elmondható, hogy az Egyesült Államokban az adatbiztonsággal, a hálózatbiztonsággal és az információbiztonsággal kapcsolatos jogi környezet összetett és folyamatosan fejlődik, és új törvények és szabályozások kerülnek bevezetésre a felmerülő fenyegetések és technológiák kezelésére.

Európai Unió (EU):

Az EU számos kiberbiztonsági politikát és stratégiát hozott létre, például az Európai Unió kiberbiztonsági stratégiáját, amelyek célja a hálózatok és információs rendszerek biztonságának fokozása az EU-ban.

Az EU számos jogi szabályt hozott létre a kiberbiztonsággal kapcsolatban. Ezek tartalmazzák:

- Általános adatvédelmi rendelet (GDPR): Ez a rendelet határozza meg a személyes adatok gyűjtésére, felhasználására és védelmére vonatkozó szabályokat az EU-n belül. Megköveteli a vállalatoktól, hogy tegyenek megfelelő intézkedéseket a személyes adatok védelme érdekében a jogosulatlan hozzáférés, megváltoztatás és ellopás ellen.
- Hálózat- és információbiztonsági irányelv (NIS-irányelv): Ez az irányelv előírja az EU-tagállamoknak, hogy hozzanak létre nemzeti kiberbiztonsági stratégiákat, és azonosítsák országukban a kritikus infrastruktúra-üzemeltetőket. Azt is előírja, hogy ezek az üzemeltetők jelentsék a nagyobb biztonsági eseményeket a nemzeti hatóságoknak.
- Kiberbiztonsági törvény: Ez a törvény keretet hoz létre az IKT-termékek és -szolgáltatások EU-szintű tanúsítási rendszerei számára. Ezenkívül létrehoz egy európai kiberbiztonsági tanúsítási csoportot és egy európai kiberbiztonsági kompetencia központot a tanúsítás felügyeletére, valamint a kiberbiztonsági kutatás és innováció koordinálására.
- eIDAS rendelet: Ez a rendelet keretet hoz létre az elektronikus azonosítás és hitelesítés EU-szerte történő elismerésére. Célja a határokon átnyúló elektronikus tranzakciók megkönnyítése, valamint az online interakciókba vetett bizalom és biztonság fokozása.

A NIS-irányelv (Directive on Security of Network and Information Systems) egy kiberbiztonsági irányelv, amelyet az Európai Unió (EU) 2016-ban fogadott el. A biztonsági kihívások hatékony kezelése EU-szintű globális megközelítést igényel, amit az irányelvnek el kell érnie. biztosítják egyfajta jogi keret biztosításával (Böröcz 2021). Célja a hálózati és információs rendszerek magas szintű kiberbiztonságának biztosítása EU-szerte. Az irányelv előírja a tagállamoknak, hogy hozzanak létre nemzeti kereteket a kiberbiztonsági kockázatok kezelésére és a kibertámadások megelőzésére, valamint jelöljenek ki illetékes hatóságokat a végrehajtás felügyeletére.

A NIS-irányelv az alapvető szolgáltatások (például energia, szállítás, banki szolgáltatások és egészségügy) üzemeltetőire és a digitális szolgáltatókra (például online piacterekre, keresőmotorokra és számítási felhő szolgáltatásokra) vonatkozik. Ezeknek a szervezeteknek megfelelő és arányos biztonsági intézkedéseket kell hozniuk a kiberkockázatok kezelése érdekében, és jelenteniük kell a jelentős incidenseket az illetékes nemzeti hatóságnak.

Az irányelv azt is előírja a tagállamok számára, hogy működjenek együtt és cseréljenek információt a kiberbiztonsági incidensekkel kapcsolatban, és hozzanak létre egy CSIRT-hálózatot (Computer Security Incident Response Team) a hatékony incidensreagálás és -kezelés érdekében (Fekete-Karydis, Lázár 2019).

A tagállamoknak 2018 májusáig át kellett ültetniük nemzeti jogukba a NIS-irányelvet, és 2018 novemberéig végre kellett hajtaniuk az irányelvet. Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) iránymutatást és támogatást nyújt a tagállamoknak az irányelv végrehajtásához.

A NIS-irányelv lényeges lépés egy biztonságosabb és ellenállóbb digitális környezet kialakítása felé az EU-ban. Segít biztosítani, hogy a kritikus infrastruktúra és a digitális szolgáltatások védve legyenek a

kiberfenyegetésekkel szemben, ezáltal minimalizálva a kibertámadások kockázatát, valamint azok társadalomra és gazdaságra gyakorolt lehetséges hatását.

Magyarország

A számítógépes hálózatok biztonságát több magyar törvény szabályozza. Az alábbiakban összefoglaljuk a legfontosabbakat:

- Büntető Törvénykönyv (Btk.): Az 1990. évi IV. törvény 353/A. §-a bünteti a jogosulatlan adatmódosítást, az adathordozó jogosulatlan felhasználását, a jogosulatlan adatszolgáltatást és a rendszer megrongálását.
- Elektronikus hírközlési törvény (2003. évi C. törvény): Ez a törvény szabályozza az elektronikus hírközlés területét, beleértve az adatbiztonsági és adatvédelmi szabályokat.
- Az információs önrendelkezési jogról és az információszabadságról szóló törvény (2011. évi CXII. törvény): Ez a törvény határozza meg az információszabadságot és az információs önrendelkezés jogi kereteit. Az adatvédelem és az adatbiztonság is fontos eleme ennek a jogszabálynak.
- Törvény a közérdekű adatok nyilvánosságáról (2011. évi CLXVI. törvény): Jelen törvény biztosítja a közérdekű adatok nyilvánosságát és hozzáférhetőségét a jogi és természetes személyek számára.
- 2013 "L." törvény: az állami és önkormányzati szervek elektronikus információbiztonságáról:
  Ez a törvény szabályozza az állami és önkormányzati szervek elektronikus információbiztonságát Magyarországon. A törvény alapvetően az állami és önkormányzati szervezetekre vonatkozik, de rendelkezéseinek hatálya kiterjed az államháztartási szervezetekre, valamint azok gazdasági társaságaira és egyéb jogi személyekre is, amelyek közpénz felhasználására jogosultak. A törvény kötelezővé teszi az állami és önkormányzati szervezetek számára az adatvédelmi és adatbiztonsági követelményeknek megfelelően szükséges biztonsági szintek meghatározását és az előírások betartását. A törvény azt is előírja, hogy az állami és önkormányzati szervezetek rendszeresen végezzenek felméréseket és auditokat a biztonsági előírások betartásának ellenőrzésére.
- Adatvédelmi törvény (2018. évi XXVIII. törvény): Jelen törvény a GDPR rendelet végrehajtását szolgáló magyar jogszabály, amely az adatvédelmi kötelezettségeket, az adatkezelők és adatfeldolgozók jogait és kötelezettségeit szabályozza.
- Ezeken a törvényeken kívül számos egyéb törvény és rendelet ír elő a számítógépes hálózatok biztonságával kapcsolatos szabályozást.

A 2013. évi L. törvény rendelkezéseket fogalmaz meg a nemzeti elektronikus adatvagyon védelmére, hiszen "Társadalmi elvárás, hogy az állam és állampolgárai olyan elektronikus információs rendszerekben legyenek kezelve, amelyek elengedhetetlenek a zárt, teljes, folyamatos és kockázatarányos az adatok és információk bizalmasságának, integritásának és elérhetőségének, valamint rendszerelemeik integritásának és elérhetőségének védelme, ezáltal védve a kiberteret." (Csordas J. 2020)

A Nemzeti Kibervédelmi Intézet (NKI) 2015-ben alakult. Az NKI biztosítja:

„A rendezvényszervezési feladatokat létfontosságú információs rendszerek és rendszerelemek, valamint

- az elektronikus kereskedelmi szolgáltatások és az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. A jogszabályi bejelentési kötelezettséggel rendelkező szolgáltatásokat nyújtó szolgáltatók esetében - így az online piacterek, internetes keresőszolgáltatások, felhőszolgáltatások - rendezvényszervezés és hatósági felügyelet."

Magyarország Nemzeti Kiberbiztonsági Stratégiája (2013):

Az Alaptörvény megközelítésével párhuzamosan szükségessé vált egy általános kibervédelmi stratégia megalkotása, amely a kibertér biztonsági szegmenseit figyelembe véve olyan alapvető és átfogó feladatokat határoz meg, amelyekkel Magyarország kibervédelmi szervei hatékonyan tudnak fellépni a kiberfenyegetésekkel szemben. A 2012-es Nemzetbiztonsági Stratégia (NBS) már nagy figyelmet fordít a kibertérre, kritikus területként jelölve meg. Magyarország Nemzeti Kiberbiztonsági Stratégiája (MNKS) célja a magyar kibertér védelme, amely a társadalmi és gazdasági élet meghatározó részét képezi, és amelyet biztonságossá kell tenni (B. Gábor 2018).

Magyarország Hálózat- és Információbiztonsági Stratégiája (2018):

A 21. században drasztikusan megnőtt a kibertámadások száma, amelyek megfékezése komoly kihívás Magyarország állami és gazdasági szektora számára. Az együttműködés felé való elmozdulás a stratégián is látható. Az állami szervek, a civil szféra és a védelmi szervezet közös feladata az információmegosztás, tevékenységük összehangolása, ami hatékonyabbá teszi a megelőzést, a reagálást és a felderítést. A 484/2013. (XII. 17.) Korm. rendelet létrehozta a Nemzeti Kiberbiztonsági Koordinációs Tanácsot, amely a Miniszterelnökség keretében valósítja meg az ágazati és kormányzati források együttes felhasználását igénylő kormányközi koordinációt (Kovács, 2020).

Számos intézmény működik együtt a Tanács koordinálásában (Sáfrán J. 2022):

- Nemzeti Kibervédelmi Intézet (NKI);
- Kormányzati Incidenskezelő Központ (GovCERT-Magyarország);
- Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);
- Információs Iroda független eseménykezelő (IntCERT);
- A Katonai Nemzetbiztonsági Szolgálat független incidensmenedzsere;
- BM Országos Katasztrófavédelmi Főigazgatóság (BM OKF/LRLIBEK);
- Magyar Tudományos Akadémia – Számítástechnikai és Automatizálási Kutatóintézet
- információbiztonsági incidenskezelő szervezetet (HunCERT) működtet;
- A Kormányzati Informatikai Fejlesztési Ügynökség (NIIF CSIRT) számítógép-biztonsági incidenskezelési szervezete.

A Kormányzati Incidenskezelő Központ (GovCERT-Hungary), amely a kibertérből származó támadásokkal és fenyegetésekkel foglalkozó incidenskezelés szakterülete, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), amely az ellenőrzéssel és végrehajtással foglalkozó hivatalos

szakterület. törvényi szabályozás, valamint az NKI szervezetén belül létrejött a kibervédelmi képességek fejlesztését és működtetését támogató, az EMIR és a FAIR rendszerek elektronikus információbiztonsági feladatait is ellátó Biztonságkezelési és Sebezhetőség Tesztelési Osztály (Kovács 2020).

A Hálózat- és Információbiztonsági Stratégia célja a hazai hálózat- és információbiztonság prioritásainak, valamint a kapcsolódó stratégiáknak és intézkedéseknek a meghatározása. A stratégia az átfogó védelmi ciklus (felderítés, megelőzés, védekezés, helyreállítás) alkalmazására összpontosít.

A stratégia legfontosabb területei:

- Az állami információs rendszerek biztonságának garantálása
- A kritikus infrastruktúrák biztonságának fenntartása
- Személyes adatok védelme
- Az elektronikus szolgáltatások biztonságának biztosítása
- A hálózat- és információbiztonsági tudatosság növelése
- A nemzetközi együttműködés erősítése a hálózat- és információbiztonság területén

A hálózatbiztonsággal kapcsolatos szabályokat az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló "233/2013. (VI. 30.)" Korm. rendelet tartalmazza (Bognár, Kátai, Vass 2014).

Jogi szabályozás összehasonlítása

Először nézzük meg az USA és az EU jogi szabályozási rendszerei közötti legfontosabb különbségeket.

Számos lényeges különbség van az EU és az Egyesült Államok hálózatbiztonsági jogszabályai között:

- Hatály: Az EU hálózatbiztonsági jogszabályokkal kapcsolatos megközelítése általában átfogóbb, mint az Egyesült Államoké. Például az EU NIS-irányelve minden „alapvető szolgáltatásra” vonatkozik, beleértve nemcsak a kritikus infrastruktúrát, hanem más típusú szolgáltatásokat is, például az online piactereket és a keresőmotorokat. Ezzel szemben az Egyesült Államok inkább szűkebben összpontosít a kritikus infrastrukturális ágazatokra, mint például az energetika és a szállítmányozás.
- Végrehajtás: Az EU általában jobban támaszkodik a hálózatbiztonsági jogszabályok szabályozási felügyeletére és betartatására, míg az USA inkább az önkéntes ipari szabványokra és az önszabályozásra támaszkodik. Például az EU általános adatvédelmi rendelete (GDPR) jelentős bírságokat szab ki a törvényi szabályozás be nem tartásáért, míg az Egyesült Államok adatbiztonsági szabályozása, például az egészségbiztosítási hordozhatóságról és elszámoltathatóságról szóló törvény (HIPAA) inkább az iparági önszabályozásra és a magánperek általi végrehajtásra támaszkodik.
- Adatvédelem: Az EU hálózatbiztonsági jogszabályaiban nagyobb hangsúlyt fektet a magánélet védelmére és az adatvédelemre, mint az Egyesült Államok. A GDPR például megköveteli a szervezetektől, hogy személyes adataik gyűjtése előtt kifejezett hozzájárulást kérjenek az egyénektől, és jogot biztosít az egyéneknek adataik törlésének kérésére. Ezzel szemben az Egyesült Államok

adatvédelmi törvényeit, mint például az Electronic Communications Privacy Act (ECPA) általában gyengébbnek és széttagoltabbnak tekintik.

- Nemzetközi hatás: Az EU hálózatbiztonsági jogszabályai, mint például a GDPR és a NIS-irányelv, jelentős hatással vannak az EU-n kívüli vállalatokra és szervezetekre, amelyek uniós polgárok adatait dolgozzák fel vagy tárolják, vagy alapvető szolgáltatásokat nyújtanak az EU-n belül. Ezzel szemben az Egyesült Államok hálózatbiztonsági jogszabályai általában kisebb hatással vannak az Egyesült Államokon kívüli területekre.

Európai Uniós tagságából adódóan a magyar adatbiztonsági, hálózatbiztonsági és információbiztonsági jogszabályoknak meg kell felelniük az Unió követelményeinek, de a nemzeti hatáskörbe tartozó kérdésekben vannak eltérések:

- Szabályozó szervek: Az EU-ban minden tagállam köteles létrehozni egy illetékes hálózat- és információbiztonsági hatóságot. Magyarországon a Nemzeti Kiberbiztonsági Központ (NCSK) feladata a nemzeti kiberbiztonsági intézkedések koordinálása.
- Szankciók: Magyarországon a hálózatbiztonsági előírások megsértésének büntetése szigorúbb, mint az EU-ban. Például a biztonsági incidens bejelentésének elmulasztásáért kiszabható maximális büntetés a magyar jogszabályok szerint lényegesen magasabb, mint az uniós jogszabályok szerint.
- Megfelelőségi követelmények: Az uniós jogszabályok részletes követelményeket fogalmaznak meg a hálózati és információs rendszerek biztonságának biztosítására, míg a magyar jogszabályok nagyobb rugalmasságot biztosítanak a szervezetek számára saját biztonsági intézkedéseik meghatározásában, amennyiben azok megfelelnek bizonyos minimumkövetelményeknek.

Főbb különbségek a magyar és az izraeli hálózatbiztonsági jogszabályok között:

- A kiberbiztonság megközelítése: Izrael proaktív megközelítést alkalmaz a kiberbiztonsággal kapcsolatban, nagy hangsúlyt fektetve a kiberbiztonsági technológiák kutatásába és fejlesztésébe, valamint a kiberbiztonsági szakemberek képzésébe történő befektetésre. Ezzel szemben Magyarország kiberbiztonsági megközelítése reaktívabb, nagyobb hangsúlyt fektet a szabályozások és szabványok betartására és betartatására.
- Szabályozási keret: Izrael átfogó jogi kerettel rendelkezik a kiberbiztonságra vonatkozóan, amely kötelező és önkéntes szabályozásokat is tartalmaz, például a kibervédelmi törvényt, az adatvédelmi szabályzatot és a létfontosságú infrastruktúrák védelméről szóló szabályzatot. Magyarország kiberbiztonsági jogi kerete még alakulóban van, a legrelevánsabb törvények az Elektronikus információbiztonságról szóló törvény és az elektronikus kereskedelemről és az információs társadalom szolgáltatásairól szóló törvény.
- Együttműködés nemzetközi partnerekkel: Izrael erős partneri kapcsolatokat épített ki az Egyesült Államokkal és más országokkal a kiberbiztonsági kutatás és fejlesztés, a hírszerzési adatok megosztása és a közös képzési gyakorlatok területén. Magyarország ezzel szemben inkább a regionális együttműködésre helyezte a hangsúlyt az Európai Unió többi tagállamával.
- Konkrét fenyegetésekre összpontosítva: Izraelnek egyedi kiberbiztonsági kihívásokkal kell szembenéznie elhelyezkedése és geopolitikai helyzete miatt, ideértve a szomszédos országokkal fennálló folyamatos konfliktusokat és a magas szintű terrorista tevékenységet. Ennek eredményeként Izrael speciális képességeket fejlesztett ki olyan területeken, mint a kiberhírszerzés és az offenzív kiberműveletek. Magyarország inkább tipikus és általános kiberbiztonsági fenyegetésekkel néz szembe, mint például a kiberbűnözés és az adatszivárgás, amelyek más európai országokban is elterjedtek.

Összegzés

Megállapítható, hogy a szabályozási környezet folyamatosan változik, fejlődik, a jogalkotók igyekeznek lépést tartani a fejlődéssel. Izraelben a fenyegetettség magas szintje miatt a kibervédelem nagyon fejlett, és a legmagasabb szinten, közvetlenül a kormánynak alárendelve, katonai irányítás alatt működik.

Az USA-ban - ahol óriási az egységes piac, nagyon nagy összegeket fordítanak az informatikai rendszerek biztosítására - a kibervédelem szintje is nagyon magas, bár itt több független szervezet, hatóság látja el az informatikai rendszerek kibervédelmi felügyeletét.

Az EU-ban folyamatosan törekednek az egységes biztonságos informatikai szabályozásra, ugyanakkor egyes szabályok esetén rugalmasabb keretet biztosítanak a tagországok számára.

A magyar kiberbiztonsági szabályozás sok tekintetben követi a nemzetközi trendeket és az Európai Uniós irányelveket, de van még hova fejlődni, frissíteni. Magyarország 2018. évi Hálózat- és Információbiztonsági Stratégiája szerint a hazai kiberbiztonsági előírások és jogszabályok továbbfejlesztésre szorulnak, hogy megfeleljenek a nemzetközi és európai szabványoknak és irányelveknek. Ennek érdekében az ország az elmúlt években számos kiberbiztonsági stratégiát és cselekvési tervet dolgozott ki, amelyek célja az ország kiberbiztonsági képességeinek további erősítése és a jogi szabályozás aktualizálása.

A magyar szabályozási rendszerről elmondható, hogy a jogalkotók az információbiztonsági szakemberekkel együtt folyamatosan elsősorban az uniós irányelveket követik, és ezeknek megfelelően alakítják ki a hazai szabályozást, amely szerencsére nem igazán marad el a tapasztalt szinttől. a legfejlettebb országokban.

Az ukrán-orosz háború és az eszkaláció veszélye miatt hazánkban is megnövekedett a kiberfenyegetettség mértéke, ezért kiemelten fontos a kritikus infrastruktúrák adatinformatikai és hálózati biztonságának emelése, amihez a szolgáltatók konstruktív együttműködése szükséges. a kormány, a jogalkotók és az érdekelt felek.

Fontos, hogy a jogalkotók ismerjék ezeket a veszélyeket, és szorosan együttműködjenek az informatikai biztonsági szakemberekkel annak érdekében, hogy egységes, korszerű jogi környezetet alakítsanak ki, amely egyrészt segíti az informatikai rendszerek biztonságának folyamatos fejlesztését, másrészt a másrészt, amennyire a jogi lehetőségek engedik, megnehezíti a kibertámadások végrehajtását.

Hivatkozások

1. Srinivas, J., Das, AK, & Kumar, N. (2019). Kormányzati előírások a kiberbiztonság területén: keretrendszer, szabványok és ajánlások. Jövő generációs számítógépes rendszerek, 92, 178-188.
2. Khan, MJ (2023). A hálózati infrastruktúra védelme kiberbiztonsággal. World Journal of Advanced Research and Reviews, 17(2), 803-813.
3. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (2020. 04. 18.)
4. Balázs, Bognár, Kátai-Urbán Lajos, and Vass Gyula. A létfontosságú rendszerek és létesítmények védelméről szóló végrehajtás szabályozása Magyarországon. Bolyai szemle (2014)
5. Cristiano, F. (2020). Izrael: A kiberbiztonság, mint nemzeti védjegy. Routledge kézikönyv a globális kiberbiztonsági stratégiához. Abingdon: Routledge.
6. Easttom, C. (2019). A számítógépes biztonság alapjai. Pearson IT minősítés.
7. Csordás, J. (2020). Az iskolai hálózatok határvédelme. Computers & Learning, 3(1), 21-31.
8. Baezner, M. és Cordey, S. (2019). Nemzeti kiberbiztonsági stratégiák összehasonlítása – kihívások Svájc számára. ETH Zürich
9. Fekete-Karydis, K., & Lázár, B. (2019). A kibervédelmi stratégiák fejlődése, kibervédelmi kihívások, aktualitások (2.). Honvédségi Szemle–Magyar Honvédelmi Szemle, 147(5), 60-72.
10. Böröcz Miklós: Az európai IT-biztonság jelenlegi kihívásai DOI: 0.38146/BSZ.2021.12.10
11. Kovács Zoltán. "Kibervédelem és biztonság." (2020): 65-90.
12. Keszthelyi, A. L. (2015). Paradigmaváltás-biztonság-emberi tényező= Paradigm shift-security-human factor. Taylor, 7(1-2), 406-412.
13. Ali, B., & Szikora, P. (2017). Információbiztonság az Y generáció körében. Tanulmánykötet-Vállalkozásfejlesztés a XXI. században VII., 24-40.
14. Gábor, B. (2018). A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. Nemzetbiztonsági Szemle, 6(3), 5-21.
15. Sáfrán, J. A magyar nemzetbiztonsági szolgálatok feladatainak változása a XXI. században az információs társadalom tükrében. (2022).
16. Kovács Zoltán: Kibervédelem és biztonság. In: Kibervédelem a bűnügyi tudományokban. Ludovika Egyetemi Kiadó Nonprofit Kft. – Ludovika Press, Budapest, 2020
17. 484/2013. (XII. 17.) Korm. rendeletben foglaltak szerint. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről. Online: https://net.jogtar.hu/jogszabaly?docid=a1300484.kor [2021. 01.11.]
18. Megjelent Magyarország hálózati és információbiztonsági stratégiája. Jogalappal.hu. Online: https://jogalappal.hu/megjelent-magyarorszag-halozati-es-informaciobiztonsagi-strategiaja/ [2021. 01. 11
19. Megjelent Magyarország Nemzeti Biztonsági Stratégiája. Jogalappal.hu. Online:https://jogalappal.hu/megjelent-magyarorszag-nemzeti-biztonsagi-strategiaja/?fbclid=IwAR31R0-41yyxr1jah4KGyqb40YxWmFkAlopiIwGXW8sFhKTo76s0V8BCRxE [2021. 01. 11.]

20. A Kormány 1139/2013. (III. 21.) Korm. rendelet 4. -a. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról; Magyar Közlöny; 2013. évi 47. szám,