Berzsenyi Dániel

# A kiberbiztonság humán oldala[1]

*Az elmúlt években számtalan kiberbiztonsági incidens történt, amelyek között több történelmi jelentőségű esetet is találhatunk. A kiváltó okok közül csak az egyik, hogy az infokommunikációs technológia terjedésével párhuzamosan a támadási felület is növekszik, és emiatt egyre több és egyre komplexebb rendszer biztonságáról kellene gondoskodni. Az incidensek meredek növekedésének további okai között éppúgy megtalálható az alulfinanszírozottság, a tájékozatlanság, vagy a kitettség alábecslése, mint a biztonságos rendszerek tervezéséhez és azok biztonságos üzemeltetéséhez szükséges szakemberek hiánya. Utóbbival az Amerikai Egyesült Államok – vezető infokommunikációs társadalomként – már 2009-ben szembesült. A kiberbiztonság humán területeket érintő kihívásaival mára egyre több ország kénytelen szembenézni, azonban szakmai körökben is vita van a kiberbiztonsági szakemberhiány realitásáról és mértékéről. Jelen írás a szakemberhiányt reális kihívásként kezeli, és ennek tükrében nyújt betekintést a kiberbiztonsághoz kapcsolódó, humán területeket érintő problémákba, kiemelve a kezelésükre tett néhány intézkedést, amelyek bevált gyakorlati példaként szolgálhatnak.*

***Kulcsszavak:*** *kiberbiztonság, szakember, szakértelem, hiány, humánerőforrás*

***Berzsenyi Dániel: The Human Side of Cybersecurity***

*We have witnessed countless cyber security incidents in recent years, some of them of historical importance. Among their causes the increasing vulnerabilities created by spreading info-communication technologies and more complex systems that require protection is only one. Further reasons for the sharp increase in the number of cyber incidents are underfinancing, lack of knowledge, underestimated exposure, as well as the lack of skilled professionals who can design and operate secure systems. The United States, as a leading info-communication society, has faced this problem in 2009. By now, more and more countries must face the challenge of lacking human resources, still its reality and extent are debated even among professionals. The current article deems the lack of skilled professionals in this field a real phenomenon, and from this point of departure offers insights into the human resource management problems in the field of cyber security, highlighting some measures as good practices that are aimed to counter such challenges.*

***Keywords:*** *cybersecurity, professional, skills, shortage, human resources*

## Bevezetés

Mintegy három évtized telt el azóta, hogy az első kártékony számítógépes programok napvilágot láttak, azonban az átlag felhasználó számára még ma sincs sok különbség az időn-

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

ként vírusnak, féregnek vagy éppen trójainak nevezett rosszindulatú szoftverek között. Jobb esetben csak annyit tapasztalunk, hogy a számítógépre telepített biztonsági szoftver érzékel, majd szerencsés esetben semlegesít valamilyen kibertérből érkező fenyegetést, de jellemzően az incidens hátteréről éppúgy nem rendelkezünk információval, mint az azt elhárító mechanizmusról. Rosszabb esetben fel sem tűnik, hogy kibertámadás áldozataivá váltunk, egészen addig, amíg például visszaélés nem történik az eltulajdonított bankkártyaadatainkkal, vagy zsaroló üzenet nem érkezik, amelyben váltságdíjat követelnek adatainkért cserébe. Ilyenkor aztán segítséget és támogatást remélve azonnal a bankunkhoz, az internetszolgáltatónkhoz, a biztonsági szoftverünk gyártójához, esetenként a hatóságokhoz fordulunk, mert bízunk abban, hogy annak az információbiztonsági szaktudásnak a birtokában, amivel mi nem rendelkezünk, az említett szervezetek alkalmazottai képesek lesznek megoldást nyújtani problémáinkra. Napjainkban azonban a megfelelő képesítéssel és naprakész információbiztonsági ismeretekkel rendelkező személyi állomány biztosítása egyre jelentősebb kihívás elé állítja a kis- és nagyvállalatokat éppúgy, mint a kormányokat az egész világon.

Az elmúlt évek során gyakran hallhatunk arról, hogy az állami és a versenyszférában is egyre nehezebb információ-, illetve kiberbiztonsági területre megfelelő szakembert találni. A témában számos elemzést, felmérést, tudományos igényű kutatást publikáltak, amelyek árnyalják a sajtó által közvetített képet, amely szerint kritikus hiány lenne kiberbiztonsági szakértőkből. Ugyanakkor az állami szférában a szakemberhiány létező nemzetbiztonsági kockázatot jelent, miközben a versenyszférában is egyre kiélezettebb küzdelem folyik a munkaadók között a legkiválóbb szakemberekért. A helyzet kialakulásában több tényező is szerephez jutott. Egyfelől a kiberbiztonsági szakértelem iránti igény hirtelen megnövekedése felkészületlenül érte a munkaerőpiacot, másfelől az infokommunikációs technológia rendkívüli mértékű terjedése és fejlődése tovább bonyolítja a helyzetet. További problémát jelent, hogy a jelenlegi trendek alapján egyre kevesebben választanak tanulmányaik során olyan szakirányt, amely később átjárást biztosítana a kiberbiztonság világába, és egyre több országban születik olyan jogszabályi háttér, amely biztonsági felelős és más specialisták kinevezését írja elő az infokommunikációs rendszerekkel összefüggésben. A legtöbb szabályozás jellemzően komoly elvárásokat is megfogalmaz a kinevezett felelősök és specialisták ismereteire vonatkozóan, ami tovább erősíti a kiberbiztonsági szakértelem iránti keresletet. Az írás célja, hogy bemutassa a közelmúlt eredményeit a kiberbiztonság és a humántőke összefüggéseivel kapcsolatban.

## Információs műveletek és humánerőforrás

2017-ben abszolút közhelynek számít az a kijelentés, hogy az infokommunikációs technológia elterjedése, a számítógépek egyre több emberi tevékenység során történő alkalmazása és hálózatba kapcsolása olyan mértékben változtatta meg életünket, hogy egyre kevésbé vagyunk képesek tolerálni ezeknek az eszközöknek a nem megfelelő működését, leállását. Az említett intolerancia jelentős mértékben abból fakad, hogy az infokommunikációs technológiák rohamos előretörése a puszta létezéstől az utazáson és kereskedelmen át egészen a hadviselésig minden emberi tevékenységre kihat. Bár a hadviselésben már

régóta léteznek úgynevezett információs műveletek, mint például a katonai megtévesztés, a tömegtájékoztatás vagy a pszichológiai műveletek, az infokommunikációs technológia fejlődése és elterjedése ezt a területet sem hagyta érintetlenül. A számítógép-hálózati hadviselés ma már szerves részét képezi az információs műveleteknek, amelyeknek a céljai között szerepel a szemben álló fél rendszerei, hálózatai és szervezetei számára külső anyagi utánpótlást, energiát vagy vezetési információt biztosító képességeinek rombolása.[2] Más megközelítésben az információs műveleteken azt az – egyébként egymástól függetlenül is létező információs tevékenységek közötti – integrációt és koordinációt értjük, ami jelentős hatékonyságjavulást eredményez az egyes információs tevékenységek összehangolása és a szinergiák kihasználása által.[3] Az információs műveleteknek azt a szegmensét, amelynek végrehajtása a kibertérben vagy annak felhasználásával történik, kiberműveleteknek is nevezzük.

A kibertérrel kapcsolatban jelenleg eltérő nézetek uralkodnak, meghatározására vonatkozóan számos definíciót találhatunk. A KFKI hálózati kislexikonban például az alábbi megfogalmazás található: „A kibertér nem más, mint a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben."[4] Suba Ferenc, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) korábbi alelnöke a kibertér meghatározásakor fontosnak tartja, hogy „egymástól kölcsönösen függő, összekapcsolt információs rendszerek" és a „rajtuk áramló digitális információk" alkotják, továbbá részét képezik az „ezen információkkal és információs rendszerekkel kölcsönhatásba lépő felhasználók" is.[5] A kibertérben zajló tevékenységekre nagyobb hangsúlyt fektető definíciót használ Magyarország Nemzeti Kibervédelmi Stratégiája (NKVS), amely szerint „a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti".[6] A katonai megközelítést vizsgálva, Haig Zsolt és Kovács László meghatározása alapján „a kibertér a civil terminológia szerint az elektronikus kommunikációs eszközök és rendszerek, valamint a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve, amit a katonai értelmezés kiterjeszt. A kibővített katonai dimenzió magába foglal olyan harctéri elektronikai eszközöket is, mint például a rádiók, radarok, azonosító berendezések, amelyek a számítógépekkel együtt nehezen elválasztható hálózatokat alkotnak."[7] Jól érzékelhető a különböző meghatározások eltérő szempontok alapján történő megfogalmazása, azonban a kibertér főbb jellemzői így is kirajzolódnak. A kibertér olyan elektromágneses energia felhasználásával létrejövő, hálózatalapú dimenzió, amelynek felhasználóként mi magunk is részévé válunk azáltal, hogy rajta keresztül adatokat, információkat állítunk elő, szerzünk meg, tárolunk és továbbítunk. Katonai szempontból további

---

[2] Haig Zsolt – Kovács László: Fenyegetések a cybertérből, *Nemzet és Biztonság,* 1. évf., 2008/5, 63. o.

[3] Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben. Robothadviselés 5. Tudományos Konferencia kiadványa, *Bolyai Szemle,* 15. évf., 2006/1, 12. o.

[4] Hálózati kislexikon, [online], Forrás: KFKI [2017. 05. 10.].

[5] Suba Ferenc: Kiberbiztonság a világban és Magyarországon (előadás), [online], Forrás: Slideplayer.hu [2015. 02. 03.].

[6] 1139/2013. (III.21.) Korm. határozat, Magyarország Nemzeti Kibervédelmi Stratégiája, [online], *Magyar Közlöny*, 2013/47. 3. pont. [2013. 04. 02.].

[7] Haig–Kovács: *i. m*., 62.

fontos jellemzője a kibertérnek, hogy a hadviselés ötödik dimenziója, ahol a kiberműveletek zajlanak, és a kibertér átível mind a négy hagyományos (szárazföldi, légi, tengeri, kozmikus) hadszíntéren.

Bár a kiberműveletek megfogalmazás nem igazán elterjedt az általános információbiztonsági és a versenyszféra által alkalmazott terminológiában, hasonló tevékenységet a mindennapok során is megfigyelhetünk az egyre gyakrabban előforduló, eltérő eredményekkel járó kiberbiztonsági incidensek kapcsán. Ezekben az esetekben – akárcsak a hadviselés során – az egyik oldal célja az infokommunikációs rendszerek működésének befolyásolása, lerontása, lehetetlenné tétele,[8] míg a másik oldal igyekszik a rendszerek működését és sértetlenségét biztosítani. Az infokommunikációs rendszerek megfelelő működése és biztonsága ma még nagymértékben embereken múlik, akik különböző szintű kiberbiztonsági ismeretekkel rendelkeznek. Közülük az írás azokra fókuszál, akiknek a feladata biztonságos rendszereket tervezni és biztonságos programkódokat írni, részt vesznek az infokommunikációs rendszerek biztonságos üzemeltetésében, támogatást nyújtanak a felhasználók biztonsági problémáihoz, továbbá szerepet játszanak a kiberbiztonsági incidensek megelőzésében, azonosításában, elhárításában, valamint a károk felszámolásában. Az említett kiberbiztonsági szakemberek speciális tudás birtokában vannak, jóval kiterjedtebb és mélyebb ismeretekkel rendelkeznek annál, mint amire egy átlagos felhasználónak szüksége lenne ahhoz, hogy teljesítse az alapvető kiberbiztonsági higiénia elvárásait. A speciális tudás elsajátítása jellemzően különböző képzési formákban és/vagy gyakorlati tapasztalatok megszerzésével történik, azonban mindkettő időigényes folyamat. Arról, hogy a megfelelő időben a megfelelő helyen rendelkezésre álljon a szükséges – esetünkben kiberbiztonsági – szaktudás egy szervezeten belül, a humánerőforrásgazdálkodásnak kell gondoskodnia, azonban egy folyamatosan változó területen[9] nem mindig egyszerű teljesíteni az elvárásokat. A munkaerőpiac visszajelzései alapján a kiberbiztonsági pozíciók száma folyamatos növekedést mutat, miközben az állások betöltését számos probléma nehezíti. Korábban a humánerőforrás és a kiberbiztonság metszetében gondot jelentett a szükséges költségvetés hiánya, vagyis a munkaadók nem biztosítottak elegendő forrást arra, hogy jól képzett, megfelelő gyakorlattal rendelkező kiberbiztonsági szakembereket tudjanak alkalmazni. A problémát észlelve és az infokommunikációs rendszerek biztonságára költhető forrásokat megemelve mára ez a jelenség eltűnőben van, azonban más nehézségek esetében kevésbé egyszerű és kézenfekvő a megoldás.

Az infokommunikációs technológia földrajzi, társadalmi, vallási, politikai és gazdasági határokat nem ismerve feltartóztathatatlanul terjed, ahogy vele együtt a technológia biztonságos működésével kapcsolatos elvárások is. A megnövekedett igényeket a jelenlegi szakemberekkel már nem lehet kielégíteni, a megfelelő számú utánpótlás kinevelése pedig hosszabb távú folyamat, ráadásul a statisztikák alapján a műszaki és mérnöki tudományok nem tartoznak a legnépszerűbb képzési területekhez, a fejlett világban egyre kevesebben szeretnének ilyen végzettséget szerezni. Mindez jelentős hatással van az információs, illetve kiberműveletekre, hiszen a szakemberhiány az állami szférában nemcsak az utánpótlás biz-

[8] Haig: *i. m.*, 3.

[9] Karoliny Mártonné – Poór József: *Emberi erőforrás menedzsment kézikönyv. Rendszerek és alkalmazások*, 5. átdolgozott kiadás, Complex, Budapest, 2010, 27. o.

tosítása kapcsán jelent kihívást, hanem a meglévő szakemberek elvándorlására is hatással van, hiszen a versenyszféra a világon mindenütt helyzeti előnyben van a fizetések és a kapcsolódó juttatási csomag tekintetében.

## A kiberbiztonsági munkaerő helyzete

2014 nyarán a RAND Corporation kiadott egy tanulmányt H4CKER5 WANTED címmel, amely alapvetően a kiberbiztonsági munkaerő egyesült államokbeli helyzetével foglalkozott. Ha elfogadjuk, hogy az Egyesült Államokat érintő infokommunikációs technológiákkal összefüggő folyamatok – ha némi késleltetéssel is, de – érzékelhetők a világ más régióiban is, akkor a tanulmány megállapításai hasznosak lehetnek bármely ország számára. A tanulmány szerzői több korábbi jelentés és felmérés eredményét is feldolgozták, mint például az amerikai Kormányzati Ellenőrzési Hivatal *(U.S. Government Accountability Office – GAO),* az amerikai kormányzat számára tanácsadói tevékenységet folytató Booz-Allen Hamilton (BAH) vállalat, az amerikai Védelmi Minisztérium *(Department of Defense – DoD),* vagy a Belbiztonsági Tanácsadó Testület *(Homeland Security Advisory Council – HSAC)* vonatkozó anyagai. A GAO az azóta a történelem egyik legjelentősebb adatlopási incidensét elszenvedő kormányzati Személyzeti Irodával *(Office of Personnel Management – OPM)* közösen megfogalmazott több követendő gyakorlatot is a kiberbiztonsági munkaerő utánpótlásával kapcsolatban. A GAO munkatársai felhívták a figyelmet a nemzetbiztonsági átvilágításokból fakadó anomáliákra, amelyek miatt akár egy évig is elhúzódhatott egy felvételi procedúra, és listázták azokat a kormányzati kezdeményezéseket, amelyek a különböző állami szervezetek számára nyújtanak segítséget a megfelelő kiberbiztonsági munkaerő megtalálásában és képzésében.[10]

Az OPM-hez hasonlóan ismerős lehet a Booz-Allen Hamilton vállalat neve is, mivel ez volt az a cég, amely munkaerő-kölcsönzés keretében Edward Snowdent kiközvetítette az amerikai Nemzetbiztonsági Szolgálathoz *(National Security Agency – NSA),* ahol ennek következtében 2013-ban Snowdennek lehetősége nyílt leleplezni az amerikai titkosszolgálatok tömeges megfigyelési gyakorlatát. A BAH is készített korábban egy gyakran hivatkozott tanulmányt arról, hogy milyen elvek és módszerek mentén lehetne erősíteni az amerikai szövetségi hivatalok kiberbiztonsági munkaerő állományát. A tanulmány szerzői többek között megállapították, hogy az amerikai kormányzati kiberbiztonsági munkaerőprogramok széttagoltak, az OPM tevékenysége nem megfelelő, az alkalmazási szabályok túl komplexek, miközben a megbízásos szerződéssel történő alkalmazás jóval egyszerűbb. A szolgálatért kapott ösztöndíjprogramok sem jártak teljes sikerrel, az állami szervezetek pedig egymás elől vették el a kiberbiztonsági szakembereket, miközben továbbra sem jutott elegendő pénz kiberbiztonsági képzésre és humánerőforrás-fejlesztésre.[11]

A Stratégiai és Nemzetközi Tanulmányok Központ *(Center for Strategic and International Studies – CSIS)* kiberbiztonsági munkaerővel foglalkozó elemzése alapvetően nem pénzügyi problémákat állapított meg az amerikai kormányzat szakemberhiányával kapcso-

[10] Martin C. Libicki – David Senty – Julia Pollak: *H4CKER5 WANTED, An Examination of the Cybersecurity Labor Market*, [online], 2014, 24–25. o. Forrás: RAND Corporation. [2014. 06. 23.].

[11] Uo.

latban, hanem sokkal inkább a menedzsment alacsony hatékonyságát hibáztatta a kialakult helyzetért. A legfontosabb javaslatok között szerepelt az amerikai Belbiztonsági Minisztérium *(Department of Homeland Security – DHS)* számára a kibertérhez kapcsolódó kormányzati szerepkörök és szakismeretek rendszertanának kialakítása, az amerikai Nemzeti Szabványügyi és Technológiai Intézet *(National Institute of Standards and Technology)* és más szereplők számára az engedélyezési követelményrendszer létrehozása, valamint az OPM számára a karrierstruktúra javítása.[12]

Az amerikai Védelmi Minisztérium jelentése a kiberműveletek személyi állományáról jelentős létszámhiányt mutatott ki, illetve felhívta a figyelmet arra, hogy a különböző szolgálati ágaknak és haderőelemeknek eltérők az igényei a kiberbiztonsági szakértelem terén. A minisztérium több programot is indított, hogy a DoD alá tartozó szervezetekben csökkenteni lehessen a kiberbiztonsági szakemberek hiányát, amelyek elsősorban a képzési feltételek javítását és a pénzügyi körülmények fejlesztését szolgálták, például az iCollege program létrehozásával, vagy a szakmai tanúsítványokért járó bónuszrendszer kialakításával.[13]

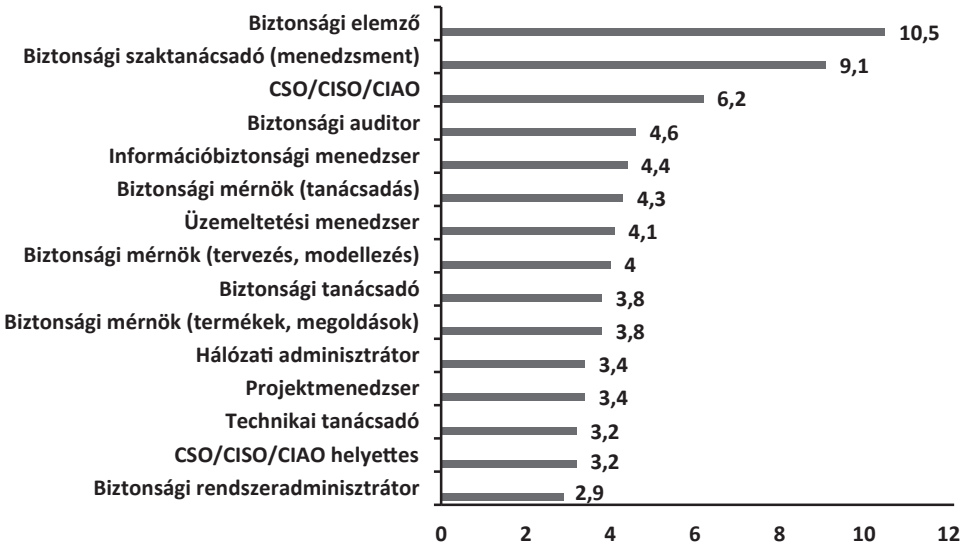
A Belbiztonsági Tanácsadó Testület (HSAC) létrehozott egy munkacsoportot, amelynek olyan kiemelkedő személyiségek is tagjai voltak, mint például Jeff Moss, a DEF CON hackerkonferencia alapítója, vagy Alan Paller, a SANS Intézetet vezetője. A testület arra jutott, hogy a Belbiztonsági Minisztérium (DHS) versenyképtelenné vált a munkaerőpiacon, mivel nem volt képes kellően érdekes és kihívásokkal teli munkát kínálni a kiberbiztonsági szakemberek számára. Az amerikai kormányzat számára megfogalmazott legfontosabb javaslatok:

– irányadó lista elkészítése a kritikus kormányzati kiberbiztonsági feladatokról;
– gyakorlati forgatókönyvek és egy értékelési modell kifejlesztése;
– dedikált tanácsadó testület felállítása a kiberbiztonsági munkaerő fejlesztésére;
– a veteránok bevonása és kiberbiztonsági tartalékos program kialakítása.[14]

A kiberbiztonsági feladatokat és a kapcsolódó munkaköröket általában egy kategóriába sorolva emlegetik, azonban rendkívül szerteágazó tevékenységet fednek le a kiberbiztonsági pozíciók, így a szükséges szaktudás is eltérő. Bizonyos munkakörök betöltéséhez elengedhetetlen az erős technikai háttér, adott esetben a mérnöki végzettség, míg más esetekben inkább menedzsmentismeretekre és vezetői képességekre, úgynevezett „soft skillekre" van szükség. Az (ISC)[2] a világ egyik legnagyobb, információ- és szoftverbiztonsági szakembereket tömörítő szervezete, amelynek több mint 160 országból 100 ezernél is több tagja van. A szervezet által készített felmérés szerint 2015-ben a kiberbiztonság területén dolgozók több mint 10%-a biztonsági elemző volt, 9% körül alakult a biztonsági tanácsadók aránya, illetve meghaladta a 6%-ot a biztonsági és információbiztonsági vezetők aránya.

[12] Uo., 19–22.
[13] Uo., 22–24.
[14] Uo., 24–25.

**1. ábra: Kiberbiztonsági munkaköröket betöltő szakemberek megoszlása 2015-ben[15]**

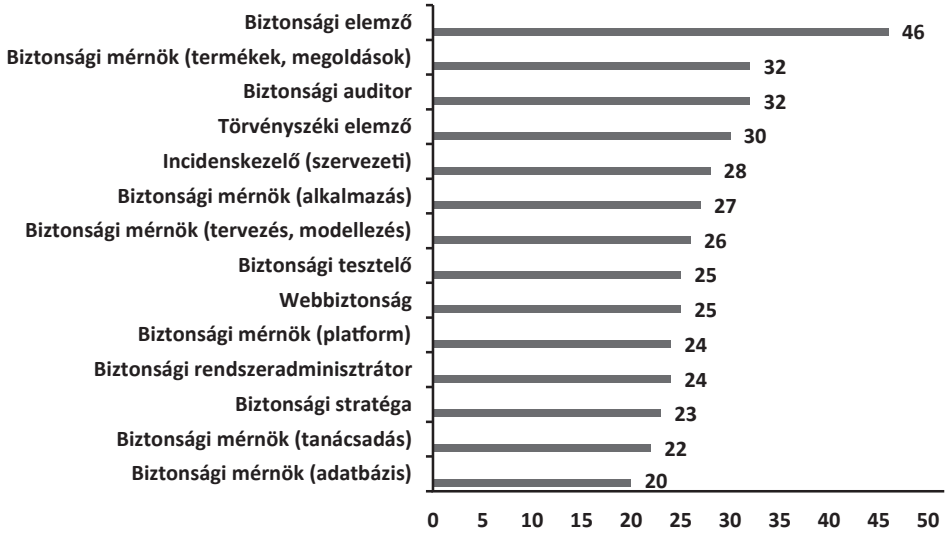



*Forrás:* Michael Suby – Frank Dickson: The 2015 (ISC)² Global Information Security Workforce Study, [online], Frost & Sullivan, 2015, 21. o. [2015. 05. 21.]. Az eredeti forrás felhasználásával szerkesztette és fordította a szerző.

A felmérés készítői arra is kíváncsiak voltak, hogy azoknál a szervezeteknél, ahol a válaszadók dolgoznak, milyen kiberbiztonsági szakmákban van hiány, illetve melyik pozíciók feltöltése jelenti a legnagyobb kihívást. Az eredmények azt mutatják, hogy bár a válaszadók között is jelentős számban vannak a biztonsági elemzők, még többre lenne szükség. A legnagyobb, közel 50%-os igény a biztonsági elemzők iránt mutatkozik, de egyformán keresettek a biztonsági auditorok és azok a mérnökök, akik a biztonsági termékek és megoldások tervezéséért felelősek.

[15] Az (ISC)² számára készített 2015-ös felmérésben 14 ezer válaszadó szerepelt; a kapott eredményből következtetni lehet a globális viszonyokra is.

**2. ábra: A legkeresettebb kiberbiztonsági szakmák sorrendje**

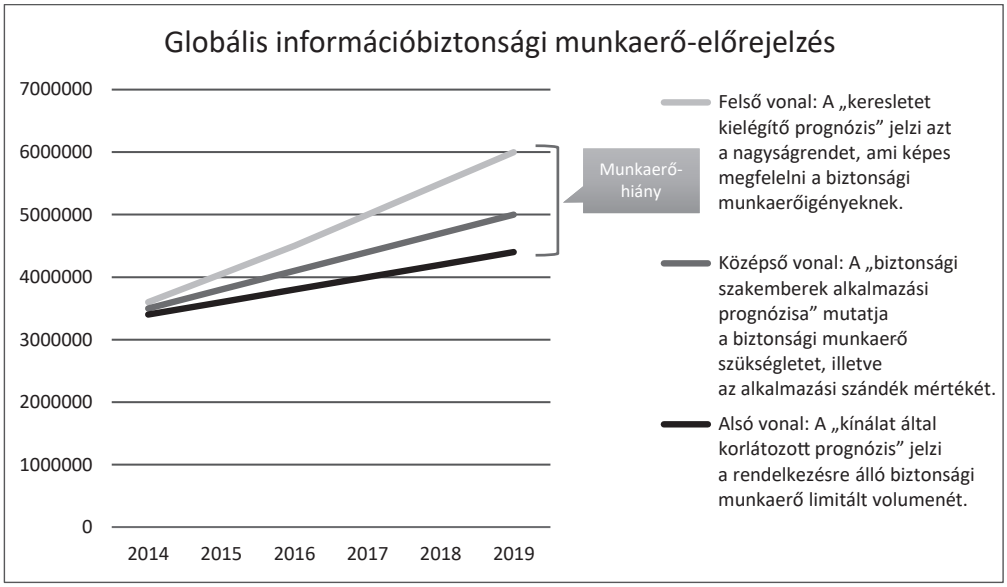



*Forrás:* Suby–Dickson: *i. m.,* 28. Az eredeti forrás felhasználásával szerkesztette és fordította a szerző.

A válaszokból kitűnik, hogy jelentős igény van törvényszéki, illetve nyombiztosító elemzőkre, incidensek kezelésében jártas szakemberekre, de keresettek a biztonsági tesztelők, illetve az adatbázisok, az alkalmazások és a különböző platformok biztonságához értő mérnökök is.

A 2015-ös felmérés alapján a készítők egy 2014–2019 közötti időszakra vonatkozó becslést is elvégeztek, amiből jól látszik, hogy a nagyjából 3,5 milliós szakemberlétszám 2019-re 4,5 millió körülire bővül, azonban az igények ennél jóval nagyobb mértékben fognak növekedni: globális szinten a kereslet várhatóan eléri a 6 millió főt. A mintegy 1,5 millió fős különbség olyan kihívást jelent humán oldalról a kiberbiztonságban, amire ma még nem tudjuk biztosan a válaszokat. Amit viszont már most is biztosan tudunk, hogy erre a kihívásra egyetlen ember vagy szervezet nem lesz képes válaszokat adni. A kiberbiztonsági közösségnek és minden a kibertérrel kapcsolatba kerülő szervezetnek közre kell működnie abban, hogy a biztonság nagyobb figyelmet kapjon az átlag felhasználók körében éppúgy, mint a pályaválasztás előtt álló fiatalok esetében. A szükséges lépések késése vagy elmaradása csak ronthat a helyzeten.

**3. ábra: A kiberbiztonsági munkaerő várható alakulása 2014 és 2019 között[16]**




*Forrás:* Suby–Dickson: *i. m.,* 32. Az eredeti forrás felhasználásával szerkesztette és fordította a szerző.

Jól látható, hogy miközben a kiberbiztonsági munkaerő hiánya valamennyi szektort érinti, még az Amerikai Egyesült Államok kormánya számára is komoly nehézségeket okoz a helyzet megoldása. Az USA kormányának rendszerszintű problémákkal kell szembenéznie, és bár a munkát más országok kormányaihoz képest jóval korábban megkezdték, úgy tűnik, a helyzet javítása rendkívül lassan halad. Elég csak a korábban már említett OPM-adatlopási botrányra gondolni, amelyet 2015 júniusában fedeztek fel az illetékesek, és több mint 22 millió főt, az Egyesült Államok lakosságának 7%-át érintette az ügy.[17] Szintén beszédes adatokat mutat a Raytheon amerikai védelmi ipari vállalat támogatásával az amerikai Nemzeti Kiberbiztonsági Szövetség *(National Cyber Security Alliance – NCSA)* által készített felmérés, amely elsősorban az Y-generáció tagjai között vizsgálta a kiberbiztonsági szakma iránti érdeklődést. A felmérési eredményekből kitűnik, hogy a Közel-Keletet leszámítva minden régióban, illetve globálisan is 60% felett van azoknak a fiataloknak a száma, akik számára soha senki nem vetette fel annak lehetőségét, hogy kiberbiztonsági karriert építsenek, ugyanakkor a válaszadók 38%-a szeretne többet tudni a terület karrierlehetőségeiről. Szintén rendszerszintű problémára mutat rá, hogy globális szinten a fiatalok 58%-a nem részesült kiberbiztonsággal kapcsolatos formális oktatásban.[18]

[16] Az alsóvonal jelöli azt a létszámot, amely biztosan megjelenik kínálati oldalon, a középső vonal mutatja az alkalmazási szándék várható alakulását, míg a felső vonal azt jelzi, hogy mekkora lesz a teljes munkaerőigény a kiberbiztonság terén.

[17] Patricia Zengerle – Megan Casella: *Millions more Americans hit by government personnel data hack*, [online], 2015. 07. 09. Forrás: Reuters [2015. 07. 10.].

[18] *Securing Our Future: Closing the Cybersecurity Talent Gap,* [online], 2015. 08. 09., 5. o. Forrás: Raytheon.com [2016. 10. 30.].

Az ISC²-hez hasonló nemzetközi szakmai szervezet az Information Systems Audit and Control Association (ISACA), amely a 2016-ban tagjai körében végzett felmérés[19] alapján több megállapítással is szolgál a 2017-es kiberbiztonsági munkaerő terén kialakult helyzetre vonatkozóan. A felmérés eredményeit közlő dokumentum szerint az információ- és kiberbiztonsági szakemberek iránti igény folyamatos növekedést mutat, miközben a munkaerőhiány ezen a specifikus területen olyan makacsul jelen van, hogy az közvetlen és mérhető károkat okoz napjaink hálózati alapon működő szervezetei számára. A felmérésből kinyert statisztikák meglehetősen negatív képet közvetítenek. Ezek alapján 2017-ben a nyitott információ- és kiberbiztonsági pozíciók betöltése a szervezetek 55%-a számára legalább három hónapot fog igénybe venni, de 32% esetében ez akár a hat hónapot is meghaladhatja. A kiberbiztonsági munkaerő fejlesztésében gondolkodó szervezetek számára szintén elgondolkodtató adat, hogy mindössze 13%-uk mondhatja el magáról, hogy húszan vagy annál többen jelentkeztek egy meghirdetett kiberbiztonsági állásra, miközben a szervezetek 35%-a szerint a jelentkezők kevesebb mint negyede tekinthető megfelelően kvalifikáltnak. Ebben a tekintetben a munkavállalók sincsenek könnyű helyzetben, mivel a kvalifikált jelentkező ismérve a kiberbiztonság terén a technikai tudás és a gyakorlati tapasztalat mellett a különböző szakmai tanúsítványok megléte. Előbbiek megszerzése nem egyik napról a másikra történik, ezért a potenciális jelentkezőnek hosszabb időre van szüksége, hogy ennek a kritériumnak megfeleljen, míg a tanúsítványok esetében a meglehetősen magas költségvonzat befolyásolja negatívan, hogy a kiberbiztonság iránt érdeklődő munkavállaló megfelelően kvalifikáltnak minősüljön a munkaadó számára. Összesen a válaszadók 69%-a nyilatkozott úgy, miszerint a kiberbiztonsági pozíciók esetében elvárás, hogy valamilyen szakmai tanúsítvánnyal rendelkezzen a jelentkező. A tanúsítványok magas elismertségét jól mutatja, hogy a felmérésben részt vevők nagy része ugyanolyan fontosnak vagy még fontosabbnak tartja őket, mint a hagyományos oktatást.

Az ISACA következtetéseihez nagyon hasonló álláspontot képvisel a McAfee biztonsági cég és a Center for Strategic and International Studies (CSIS) által szintén 2016-ban készített jelentés.[20] A nyolc ország (Ausztrália, Franciaország, Németország, Izrael, Japán, Mexikó, Egyesült Királyság, Amerikai Egyesült Államok) kiválasztásával készült tanulmány kritikus sérülékenységnek ítéli a kiberbiztonsági szakemberhiányt a vállalatok és a nemzetállamok számára egyaránt. Az eredmények azt mutatják, hogy a felmérésben részt vevő országokban kivétel nélkül hiányos a kiberbiztonsági oktatás, illetve a válaszadók 82%-a szerint komoly szakértelemhiánnyal kell szembenézniük. Szintén magas (76%) azoknak az aránya, akik szerint a kormányok nem fordítanak elegendő erőforrást a kiberbiztonsági képzésre és tehetséggondozásra. A felmérésben részt vevők közül minden harmadik válaszadó gondolja úgy, hogy a szakértelem hiánya vonzóbb célponttá teszi a szervezetét a rosszindulatú felhasználók számára, míg minden negyedik válaszadó számolt be arról, hogy a nem megfelelő kiberbiztonsági munkaerő alkalmazása reputációs veszteséget és közvetlen adatvesztést okozott a szervezete számára. A legkritikusabb területek a szakértelem hiánya

[19] Frank T. Downs: *State of Cyber Security 2017, Part 1: Current Trends in Workforce Development,* [online], 2017. Forrás: ISACA [2017. 02. 19.].

[20] *Hacking the Skills Shortage – A study of the international shortage in cybersecurity skills,* [online], 2016, 4. o. Forrás: McAfee – CSIS [2016. 10. 20.].

tekintetében a behatolásérzékelés, a biztonságosszoftver-fejlesztés és a támadások elhárítása, illetve a következmények enyhítése. A jelentés alapján a gyakorlati tapasztalat és a szakmai tanúsítványok megszerzése együtt hasznosabb és gyorsabb a megfelelő kiberbiztonsági szakértelem megszerzéséhez, mint egy főiskolai vagy egyetemi diploma.

## A kibertér biztonsága az oktatás és képzés tükrében

A korábban már említett 1,5 millió fős kiberbiztonsági szakemberhiány a közelmúlt eseményeinek, illetve az iparági változásoknak köszönhetően 2022-re várhatóan tovább nő, és a legújabb előrejelzések szerint globális szinten eléri az 1,8 millió főt.[21] A vonatkozó időszakban, csak Európában mintegy 350 ezer kiberbiztonsági állás lesz betöltetlen a szakértelem hiánya miatt. A rövid távon is fenntarthatatlan trendben változást idézhet elő, ha a kiberbiztonsági oktatás és képzés rendszerében mélyreható, a munkaerőpiaci elvárásoknak leginkább megfelelő változások következnek be. Figyelembe véve a korábban hivatkozott felmérések eredményeit, noha a hagyományos akadémiai intézményekre a kiberbiztonsági oktatás és képzés alapvető elemeként tekintenek a munkaadók, a nem hagyományos megoldások gyorsabb és hatékonyabb válaszokat kínálnak. A legnagyobb kihívás ezen a téren a hagyományos képzési formákat kínáló intézmények számára, hogy a gyakorlati ismeretek elsajátításának lehetőségét minél gyorsabban és eredményesebben építsék be a meglévő kiberbiztonsági programokba, illetve indítsanak a munkaerőpiaci elvárásoknak megfelelő kiberbiztonsági képzést a nulláról. Nagyjából az esetek felében egy BSc-diploma már elegendő lehet egy kiberbiztonsági pozíció elnyeréséhez, azonban a kifejezetten kiberbiztonsági képzést nyújtó intézmények és programok száma világszerte meglehetősen alacsony. Általánosságban elmondható, hogy a legjobb nevű felsőoktatási intézmények kevesebb mint 10%-a kínál a hozzájuk jelentkező hallgatók számára kiberbiztonsági oktatást. Valamivel jobb a helyzet a mesterszakok tekintetében, ahol ez az arány már eléri az egyharmadot, azonban nem szabad megfeledkeznünk arról, hogy a munkaadók egy technikai területen szerzett diplomát csak a harmadik helyre rangsorolnak a meglévő gyakorlati tapasztalatok és a szakmai tanúsítványok mögött, ha a megfelelő kiberbiztonsági szakértelem megszerzéséről van szó. Ennek tükrében egy technikai területen szerzett diploma inkább csak az általános kompetencia jele a munkaadó számára, és nem a releváns, legkeresettebb kiberbiztonsági szakértelem mutatója. A munkaadók szemében a megfelelő szakértelem vagy képesség meglétének további ismérve lehet, ha a potenciális munkaerő nemzeti és nemzetközi kiberbiztonsági, illetve hackerversenyeken indulva hívja fel magára a figyelmet. A munkaadók háromötöde gondolja úgy, hogy a kiberbiztonsági versenyek kulcsfontosságú szerepet játszanak a szakértelem fejlesztésében és a tehetségek felfedezésében.

A munkaadók részéről leginkább elfogadott alternatív oktatási és képzési lehetőségek mellett feltétlenül meg kell említeni a legújabb kezdeményezéseket, mint amilyen például az Egyesült Királyság kormánya által indított Cyber Retraining Academy,[22] amely tulaj-

[21] *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk,* [online], 2017, 3. o. Forrás: Booz Allen Hamilton – Frost & Sullivan – ISC² [2017. 02. 01.].

[22] Phil Muncaster: *Government Launches Cyber Retraining Academy,* [online], 2016. 11. 02. Forrás: InfoSecurity Magazine [2016. 11. 13.].

donképpen egy átképző intézmény, amit az ország Nemzeti Kiberbiztonsági Programja *(National Cyber Security Programme),* valamint egy neves nemzetközi kiberbiztonsági képző központ, a SANS Institute közösen működtet. Az átképzés egy intenzív 10 hetes kurzust foglal magában, amelynek az elvégzését a brit kormány jelhírszerzésért felelős szervezete, a Government Communications Headquarters (GCHQ) egy speciális tanúsítvány kiállításával ismeri el. A kezdeményezés hátterében húzódó elképzelés szerint olyan embereket szeretnének toborozni és átképezni, akik korábban nem foglalkoztak kiberbiztonsággal, de rendelkeznek azokkal a természetes adottságokkal, amelyek eredményessé tehetik őket ebben az iparágban. Az ingyenes kurzus nagy hangsúlyt fektet a rosszindulatú kódok felismerésére és a kapcsolódó gyakorlati ismeretek elsajátítására, ami egyfelől hiányzik a hagyományos képzési formákból, másfelől a munkaadók által kifejezetten keresett szakértelemnek számít. Az átképzés további különlegessége, hogy a hallgatók a biztonságos hálózatok építésén és a technikai ismereteken túl azt is megtanulják, miként gondolkodnak jövőbeli ellenfeleik az online világban. Szintén az Egyesült Királyságban indult el nemrég egy speciális online képzés, amelynek a középpontjában a humánerőforrás-gazdálkodással foglalkozó szakemberek állnak.[23] Az online kurzus célja, hogy a HR-szakemberek kiberbiztonsági ismereteit bővítsék. Az újszerű megközelítés szerint a HR-szakemberek nemcsak érzékeny adatokat kezelnek napi szinten, de felelősek a toborzásért és a munkaerő-fejlesztésért is a legtöbb szervezetben, ezért kritikus fontosságú, hogy tisztában legyenek a rájuk és a szervezetükre leselkedő kiberbiztonsági kihívásokkal és fenyegetésekkel. Az online kurzus egyfelől segíti ezen a területen dolgozókat abban, hogy saját kiberbiztonsági higiéniájukat fejlesszék, ezáltal gyorsabban és hatékonyabban detektálják a támadási kísérleteket, másfelől alaposabb ismereteket szerezhetnek a kiberbiztonsági munkaerővel szemben támasztott elvárásokról, így hatékonyabban végezhetik toborzási és szervezetfejlesztési tevékenységüket a kiberbiztonsági pozíciók tekintetében. Az ingyenes kurzus modulokból épül fel, amelyek között az általános kiberbiztonságot bemutató éppúgy megtalálható, mint a támadások kivitelezéséről és hatásairól, vagy éppen a támadások következményeinek enyhítéséről szóló elemek. Az Egyesült Királyság kormánya azonban az aktív munkavállalók mellett a fiatalabb generációt is hatékonyan szeretné motiválni a kiberbiztonsági szakmák iránt, ezért 2016 végén bejelentették, hogy a második világháborúban a kódfejtésben kulcsszerepet betöltő Bletchley Parkban megnyílik az első Nemzeti Kiberbiztonsági Iskola, amely ingyenes bentlakásos képzési lehetőséget kínál a 16–19 éves korosztály legtehetségesebb diákjai számára, hogy a jövő kiberbiztonsági vezetőivé válhassanak.[24] A mintegy 5 millió fontos projekt befejezését követően más szervezeteknek is lehetőségük nyílik majd kiberbiztonsághoz kapcsolódó rendezvényeket és képzéseket szervezni a történelmi helyszínen.

[23] Phil Muncaster: *New Government-backed HR Cybersecurity Course Launches,* [online], 2016. 02. 05. Forrás: InfoSecurity Magazine [2016. 03. 11.].

[24] Phil Muncaster: *Bletchley Park to House New National Cybersecurity College,* [online], 2016. 11. 24. Forrás: InfoSecurity Magazine [2016. 11. 26.].

## Összegzés

Bár a feldolgozott tanulmányok, jelentések és elemzések alapvetően a kiberbiztonsági munkaerő egy adott országban (például az Amerikai Egyesült Államok), vagy néhány állam alkotta csoporton belül kialakult problémájával foglalkoznak, a legtöbb olyan globális kitekintést is tartalmaz, aminek alapján bármely ország megkezdheti a trendekhez történő alkalmazkodást és a kihívásokra való felkészülést. Egyes források szerint a kiberbiztonsági szakértelem hiánya már 2016-ban olyan mértéket öltött, hogy az a kibertámadások jelentős részéért felelős kiberbűnözőket is érinti.[25] A kibertér alvilágának működési mechanizmusait és szükségleteit figyelembe véve ez egyáltalán nem meglepő, hiszen a kiberbűnözőknek komplett támadói ökoszisztémát kell fenntartaniuk a rosszindulatú kódok írására, a sérülékenységek felfedezésére, vagy éppen a botnetek üzemeltetésére. Mindez ugyanúgy mélyebb technikai ismereteket és gyakorlati tapasztalatot igényel, mint egy legális kiberbiztonsági állás. Az infokommunikációs technológiák térhódítása, a kibertér rohamos bővülése és ezáltal a kiberbiztonsági szakemberek iránti kereslet jóval nagyobb mértékű, mint amennyi kiberbiztonsági szakembert képeznek ma a világon. Ez egyfelől a specialisták fizetésének gyors és nagyarányú emelkedésével jár, másfelől egyes szervezetek számára megfizethetetlenné válik az a kiberbiztonsági szakértelem, ami az infokommunikációs rendszereik biztonságos üzemeltetéséhez szükséges lenne. A jelenlegi trendek és előrejelzések alapján a folyamat leállításával már elkésett a világ, ugyanakkor a kiberbiztonságot érintő humán jellegű kihívások kezelhetők, a negatív folyamatok lassíthatók. A szakképzett munkaerő hiányával összefüggő kiberbiztonsági kihívást elfogadható szintre lehet szorítani, amiben a technológiai fejlődés és az automatizálás térnyerése mellett elsősorban az oktatási, továbbképzési és támogatási programok bevezetése játszhat fontos szerepet. Ezen a területen néhány szervezet, illetve ország jelentős előnyre tett szert, és olyan, a hagyományos képzési formáktól eltérő megoldásokat vezetett be, amelyek követendő példaként szolgálhatnak. A főként az Amerikai Egyesült Államok és az Egyesült Királyság által indított kezdeményezések, bár országspecifikusak, a mögöttük húzódó gondolatok univerzálisak és könnyedén átültethetők más szervezetek, kormányok gyakorlatába. Különösen fontos lenne, hogy a kiberbiztonság humán kihívásaival foglalkozó szakemberek szemléletmódjába minél hamarabb, minél mélyebben beágyazódjanak a kiberbiztonsági munkaerővel szemben támasztott, piac vezérelte követelmények éppúgy, mint a szakértelem hiányára adott, új megközelítést alkalmazó, de rendszerszinten is hatékony válaszok. Ennek a szemléletmódnak és a gyors alkalmazkodás képességének rendkívüli szerepe van a kormányzati rendszerek és a kritikus információs infrastruktúrák üzemeltetőinél, hiszen esetükben a kiberbiztonsági humántőke gyengesége vagy a szakértelem hiánya nemzetbiztonsági kockázatot jelent.

[25] Dan Raywood: *Skills Shortage Hits Hackers,* [online], 2016. 11. 26. Forrás: InfoSecurity Magazine [2016. 03. 04.].

## FELHASZNÁLT IRODALOM


Downs, Frank T.: *State of Cyber Security 2017, Part 1: Current Trends in Workforce Development,* [online], 2017. Forrás: ISACA [2017. 02. 19.]

*Hacking the Skills Shortage – A study of the international shortage in cybersecurity skills,* [online], 2016. 2016, 4. Forrás: McAfee – CSIS. [2016. 10. 20.]

Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben. Robothadviselés 5. Tudományos Konferencia kiadványa, *Bolyai Szemle,* 15. évf., 2006/1, 3–12. o.

Haig Zsolt – Kovács László: Fenyegetések a cybertérből, *Nemzet és Biztonság,* 1. évf., 2008/5, 61–69. o.

Hálózati kislexikon, [online]. Forrás: KFKI [2017. 05. 10.]

Karoliny Mártonné – Poór József: *Emberi erőforrás menedzsment kézikönyv. Rendszerek és alkalmazások*, 5. átdolgozott kiadás, Complex, Budapest, 2010

Libicki, Martin C. – Senty, David – Pollak, Julia: *H4CKER5 WANTED, An Examination of the Cybersecurity Labor Market*, [online], 2014. Forrás: RAND Corporation [2014. 06. 23.]

Muncaster, Phil: *Bletchley Park to House New National Cybersecurity College,* [online], 2016. 11. 24. Forrás: InfoSecurity Magazine [2016. 11. 26.]

Muncaster, Phil: *Government Launches Cyber Retraining Academy,* [online], 2016. 11. 02. Forrás: InfoSecurity Magazine [2016. 11. 13.]

Muncaster, Phil: *New Government-backed HR Cybersecurity Course Launches,* [online], 2016. 02. 05. Forrás: InfoSecurity Magazine [2016. 03. 11.]

Raywood, Dan: *Skills Shortage Hits Hackers,* [online], 2016. 11. 26. Forrás: InfoSecurity Magazine [2016. 03. 04.]

*Securing Our Future: Closing the Cybersecurity Talent Gap,* [online], 2015. 08. 09. Forrás: Raytheon.com [2016. 10. 30.]

Suba Ferenc: Kiberbiztonság a világban és Magyarországon (előadás), [online]. Forrás: Slideplayer.hu [2015. 02. 03.]

Zengerle, Patricia – Casella, Megan: *Millions more Americans hit by government personnel data hack*, [online], 2015. 07. 09. Forrás: Reuters [2015. 07. 10.]

1139/2013. (III.21.) Korm. határozat, Magyarország Nemzeti Kibervédelmi Stratégiája, [online], *Magyar Közlöny,* 2013/47. 3. pont. [2013. 04. 02.]

*2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk,* [online], 2017. Forrás: Booz Allen Hamilton – Frost & Sullivan – ISC² [2017. 02. 01.]