HADMÉRNÖK

XIII. Évfolyam „KÖFOP” szám – 2018. január

MÉRFÖLDKÖVEK A BRIT KIBERBIZTONSÁG FEJLŐDÉSÉBEN II. INTÉZKEDÉSEK ÉS A SZERVEZETI KERETEK KIÉPÜLÉSE

MILESTONES IN THE DEVELOPMENT OF THE BRITTISH CYBER SECURITY II. MEASURES AND THE CREATION OF ORGANIZATIONAL FRAMEWORKS

MOLNÁR Dóra

(ORCID: 0000-0002-1476-5253)

molnar.dora@uni-nke.hu

Absztrakt

A tanulmány második része – építve az első részben ismertetett elméleti keretekre – azon kormányzati kereteket és intézkedéseket ismerteti, amelyeket az Egyesült Királyság az elmúlt években alakított ki kiberbiztonságának megteremtése érdekében. E körben kiemelendő a kiberbiztonsági csúcsszervként működő Nemzeti Kiberbiztonsági Központ, amely segítségével összefogják és központilag menedzselik a kiberincidensek megelőzésének és kezelésének teljes spektrumú feladatrendszerét. S bár az eredmények valóban impozánsak, azonban további biztonságnövelő intézkedések megtétele szükséges a teljes körű védelem megteremtése érdekében. Különösen igaz ez a kritikus infrastruktúra intézményei által használt rendszerekre, amelyek sérülékenysége még mindig elég magas – s ezt a 2017. évi kibertámadások is igazolják. Azonban az Egyesült Királyság a lehető legjobb úton halad ahhoz, hogy világvezető kiberállamként bármilyen kibertámadással és támadóval képes legyen felvenni a versenyt.

„A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

Kulcsszavak: *kiberbiztonság, Egyesült Királyság, Nemzeti Kiberbiztonsági Központ*

Abstract

The second part of the study –building on the theoretical framework described in the first part – reviews the governmental frameworks and measures that the United Kingdom has formed and adopted in the past few years to create its own cybersecurity. In this context, the National Cyber Security Centre as the main hub is to be emphasized, with the help of which all of the tasks concerning prevention and management of cyber incidents are joined together and centrally managed. Although the achievements are really imposing, further security building measures have to be taken to fully build the defence of the country. It is specifically true for the systems used by the institutions of the critical national infrastructure as their vulnerability is still too high – as proved by the cyberattacks against the UK in 2017. However, the United Kingdom as a leading cyber nation is on the best way to fight successfully against any kind of cyberattack or attacker.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in (the) István Egyed Postdoctoral Program.”

Keywords: *cyber security, United Kingdom, National Cyber Security Centre*

A kézirat benyújtásának dátuma (Date of the submission): 2017.10.24.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.01.13.

BEVEZETÉS

2005 óta az Egyesült Királyság teljes lakossága rendelkezik internet-hozzáféréssel, amely 99%-ban legalább 2 Mbps-os sebességet biztosít. 2013-ban már a háztartások 88%-a rendelkezett otthoni internet elérhetőséggel és a lakosság 87%-a napi szinten használta az internetet. Ezzel az Egyesült Királyság az uniós országok között a 6. helyen állt. A korcsoportonkénti bontást megnézve látható, hogy a fiatal korosztály körében kiemelkedően magas az internetet rendszeresen használók számaránya, elérve a 97%-ot a 16 és 34 év közöttiek körében. [1]

Az Egyesült Királyság azonban nem csak a lakossági online szolgáltatásokat építette ki és támogatta, hanem 1999 óta kormányzati prioritásként szerepelt az e-kormányzat megteremtése is 2008-as céldátummal. [2] Ez végül 2010-re megvalósult, és ezen túllépve mára a kitűzött cél, hogy alapesetben valamennyi kormányzati szolgáltatást digitális úton lehessen igénybe venni.[1] Ennek elérése érdekében felállították a Digitális Szolgáltatások Standardjét,[2] amely 18 kritérium alapján értékeli adott közigazgatási szolgáltatás digitális megfelelőségét.[3] [3]

Végül említést kell tenni az e-kereskedelem fontosságáról, amely arányát tekintve az egyik legmagasabb az Európai Unióban. 2013-ban a brit vállalatok 82%-a rendelkezett saját honlappal – bár az e-számlázást csak 24%-uk választotta. [5]

Összességében tehát megállapítható, hogy országszerte igen magas az internet-lefedettség aránya, de még mindig van hová fejlődni, ugyanis a kibertámadások hatalmas plusz költségeket rónak a vállalatokra. Becslések szerint egy átlagos kibertámadás okozta költségek a nagyvállalatok esetében 600.000 és 1,15 millió font közé tehetők, kisebb vállalatok esetében 65.000 font és 115.000 font közé esnek [5]. Ezért a kormányzat számos kezdeményezést indított útjára az elmúlt években, amelyek célja a vállalatok kibertámadásokkal szembeni emelt szintű védelme és az, hogy az Egyesült Királyság rugalmasan és hatékonyan tudja felvenni a küzdelmet a kiberbűnözés területén is.

Jelen tanulmány a brit kiberbiztonság korábbi, az elméleti alapokat ismertető részére építve a főbb kormányzati lépéseket és intézkedéseket mutatja be, valamint ismerteti, hogy a kiberbiztonság terén az ország milyen egyedi és hatékonynak bizonyuló lépéseket tett meg az elmúlt évek során.

A BRIT KIBERBIZTONSÁG SZERVEZETI KERETEI

A brit kiberbiztonsági szervezetrendszer *három* elkülönülő, ám egymáshoz számos ponton szorosan kapcsolódó *szervezeti elemből* tevődik össze: a politikai koordinációért és stratégiai irányvonalakért felelős kormányzati elemből, a nemzetbiztonsági szolgálatok szervezeteiből és a katonai kibervédelem intézményeiből. [6]

1. *A politikai koordinációért és stratégiai irányvonalakért felelős kormányzati elem:*

A minisztériumi jogállású központi államigazgatási szervek egyike a *Kabinetiroda* (Cabinet Office), amely a kiberbiztonság területét illetően teljes hatáskörrel bír a kormányzati koordináció és stratégiai irányvonalak kijelölése terén.[4] Ezen belül működik a *Nemzetbiztonsági Titkárság* (National Security Secretariat – NSS), amely a nemzetbiztonságot

[1] A szakirodalomban elterjedt kifejezés a „digital by default”.
[2] Digital Service Standard
[3] Ez részét képezi a Kormányzati Szolgáltatási Kézikönyvnek (Government Service Design Manual), amely segítségével a kormányzati csoportok ellenőrizni tudják, hogy a digitális szolgáltatások mennyiben felelnek meg a standardeknek. [4]
[4] Eredetileg a Belügyminisztériumi hivatal (Home Office) volt a kiberbiztonságért felelős fő kormányzati szerv, majd a jobb átláthatóság végett került át a kérdéskör felügyelete a Kabinetirodához.

érintő valamennyi kérdésben segítséget nyújt a Nemzetbiztonsági tanácsnak és a miniszterelnöknek. [7] A Titkárságon belül a *Kiberbiztonsági és Információvédelmi Iroda* (Office of Cyber Security & Information Assurance – OCSIA) foglalkozik a kiberkérdésekkel, közvetlen iránymutatásokat nyújtva a Kabinetirodát vezető miniszternek és a Nemzetbiztonsági Tanácsnak. Tevékenysége során az iroda szoros munkakapcsolatban van olyan vezető kormányzati szervekkel, mint a Védelmi Minisztérium, a Kormányzati Kommunikációs Központ (Government Communications Headquarters, a továbbiakban: GCHQ), a Nemzeti Infrastruktúravédelmi Központ (Centre for the Protection of National Infrastructure, a továbbiakban: CPNI) vagy a Külügyi és Nemzetközösségi Iroda (Foreign & Commonwealth Office). [8]

Az összkormányzati kibermegközelítés keretét kormányzati dokumentumok szintjén a 2009-es kiberstratégiában fektették le, majd a 2010-ben elfogadott Nemzetbiztonsági Stratégiában tovább finomították a négyéves *Kiberbiztonsági Program* meghirdetésével. Ahogyan arra a tanulmány első része is rámutat, a program keretében – összhangban a 2011-es kiberbiztonsági stratégiában foglaltakkal – 2011 és 2015 között több kormányzati szektort érintően történtek igen jelentős, az adott szektor kibervédelmét erősítő beruházások – kiemelve a titkosszolgálatok és a Védelmi minisztériumra eső 73%-os részesedést. [9]

2. A Nemzetbiztonsági szolgálatok szervezetei

A fent már említett *Nemzetbiztonsági Titkárság* (a Kabinetirodán belül) az összkormányzatot érintő, stratégiai titkosszolgálati kérdések koordinálásért felelős központi szervként működik. Ennek részeként az *Egyesített Titkosszolgálati Szervezet*[5] független értékeléseket készít nemzetbiztonsági vagy külpolitikai szempontból fontos kérdéseket illetően.

Központi szervként mégis a *GCHQ* szolgál. [10] A cheltenhami székhelyű[6] szervezet több, mint 6000 alkalmazottal rendelkezik és szoros a munkakapcsolata a brit titkosszolgálatok intézményeivel (kiemelten az MI5-val és az MI6-szel). Lényegében valamennyi feladata közvetlenül kapcsolódik kiberbiztonsági kérdésekhez és e területet érintően számos projektet futtat. A GCHQ részeként működik a Kibervédelmi Műveletek csoportja,[7] amely felderítő tevékenységének és elemzéseinek köszönhetően az Egyesült Királyság védelmi hálója jelentősen kiszélesedett. A GCHQ legjelentősebb alárendelt szervezete a *Nemzeti Kiberbiztonsági Központ* (National Cyber Security Centre, a továbbiakban: NCSC), amely magába olvasztotta a technikai megoldásokért felelős, korábban a GCHQ-nak alárendelten működő szervezetet, az Információbiztonsági Nemzeti Technikai Hatóságot[8] (CESG), a 2014 óta működő brit hálózatbiztonsági reagáló csoportot (CERT-UK), a Kiberértékelési Központot[9] (CCA) és a CPNI-t. (Az NCSC működésével a következő fejezet részletesen foglalkozik.) A Kiberbiztonsági Műveletek Központja[10] (CSOC) kezdetben a GCHQ szervezetén belül a kiberincidensek bekövetkezése esetén fő koordináló és ellenőrző szervként funkcionált, majd döntés született arról, hogy átalakított feladatkörrel újjászervezik, és a védelmi hálózatok és rendszerek biztonságáért fog felelni (tehát felelősségi köre alapján átkerült a katonai kibervédelem intézményei körébe). 2016. április 1-jén született döntés arról, hogy 40 millió fonttal támogatják az új központ felállítását. [11]

3. A katonai kibervédelem intézményei

[5] Joint Intelligence Organization
[6] Regionális központjai találhatók Scerborough-ban, Bude-ban, Harrogate-ben és Manchesterben.
[7] Cyber Defence Operations team
[8] National Technical Authority for Information Assurance
[9] Centre for Cyber Assessment
[10] Cyber Security Operations Centre

A katonai kibervédelem központi intézménye a *Védelmi Minisztérium*, amely a kibertér katonai célú használatáért felelős. Az Egyesült Királyság a kibertérre vonatkozó önálló védelmi stratégiával nem rendelkezik. Bár a 2011-es védelmi stratégia és a 2010-es védelmi terv sem kezelte még kiemelt prioritásként a kibervédelem kérdéskörét, ez 2015-ben megváltozott és már a stratégiai dokumentumokban is kiemelt helyen szerepel.

A katonai kiberkérdések megvalósításáért felelős másik fő szervezet a *Fegyveres erők,* amely a kiberbiztonságot az egész védelmet átható olyan területként definiálja, amely valamennyi szektort érint, és amelyet a tervezési, előkészületi és költségvetési kérdések esetében is mindig számításba kell venni. Ennek jegyében döntött úgy a vezérkari főnök, hogy az Egyesített parancsnokság alá rendeli az egyes kiberegységeket, megteremtve ezzel a kiberterületre vonatkozó konzisztens és holisztikus megközelítést. [12] A Nemzeti kiberbiztonsági program keretében a védelmi szektorba irányuló 90 millió fontot a Védelmi Kiberbiztonsági Program[11] – majd később a Védelmi kiberprogram[12] – keretében használták fel. A tevékenység négy nagy területet érintett: a kiberterület beemelése a fő kormányzati politikák közé, a Védelmi kiberműveleti csoport[13] (DCOG) felállítása, a kiberképességek fejlesztése és a jövő haderejének kiber komponenssel való ellátása.

A Védelmi Kiberbiztonsági Program keretében felállítani tervezett *Védelmi kiberműveleti csoport* létrehozásának gondolata már a 2010-ben kiadott Nemzeti biztonsági stratégiában felmerült, majd a 2011-es kiberstratégia azt már konkrétan is tartalmazta. Mire azonban a csoport ténylegesen is megkezdte működését 2013 májusában, elnevezése *Egyesített Kibercsoportra*[14] (JFCyG) változott. Ennek keretében felállítottak két egyesített kiberegységet. Az egyik Corshamban állomásozik és éjjel-nappal a Védelmi minisztérium hálózatait védi a kibertámadásoktól, míg a másik egység a GCHQ főhadiszállásán települt 2015-re és feladata, hogy új taktikákat, technikákat és terveket dolgozzon ki, amelyek segítségével a kibertérben hatékony katonai válaszadásra lesz képes az ország. [13]

Igen jelentős fejlemény volt 2013 szeptemberében az, amikor hivatalosan is bejelentették, hogy az Egyesült Királyság felállítja az *Egyesített kibertartalékos egységét.*[15] [14] Az egység feltöltését 2013 októberében kezdték meg, három személyi körből: egyrészt a fegyveres erőknél korábban szolgálatot teljesítők, másrészt a szükséges informatikai szaktudással rendelkező volt vagy még aktív tartalékosok, harmadrészt pedig olyan speciális szaktudással rendelkező szakemberek köréből, akik korábban nem teljesítettek katonai szolgálatot. Emellett további feltétel a 18. életév betöltése, a brit vagy Nemzetközösségbeli állampolgárság, különleges kibertudás igazolása, az elmúlt legalább 10 évben állandó lakóhely igazolása az Egyesült Királyság területén és a nemzetbiztonsági átvilágításon való megfelelés. [15] A tartalékosok a corshami és cheltenhami egyesített kiberegységeknek és a minisztériumhoz köthető információbiztonsági egységeknek nyújtanak szakmai támogatást.

Végül, de nem utolsósorban említést kell tenni a katonai intézményrendszer keretét adó szervezetről, a *Globális Műveletek és Biztonsági Ellenőrző Központról*[16] (GOSCC). A központ már több, mint egy évtizedes múltra tekint vissza és a brit fegyveres erők és a Védelmi minisztérium hálózatai biztonságáért felelős legfőbb intézményként funkcionál. A 24 órás szolgálatot ellátó szervezet központja a corshami minisztériumi székhelyen található. Mintegy 200.000, a védelmi szférához tartozó elektromos eszközt monitoroz, de feladatai közé tartozik

[11] Defence Cyber Security Programme
[12] Defence Cyber Programme
[13] Defence Cyber Operations Group
[14] Joint Forces Cyber Group
[15] Joint Cyber Reserve
[16] Global Operations and Security Control Cenre

a jövőbeni kibertámadásokra való felkészülés is. A központban 200-an dolgoznak, vegyesen a hadsereg állományából, a minisztérium civil szakemberi köréből és a nagy szerződéses ipari partnerek képviselőiből. [16]

A NEMZETI KIBERBIZTONSÁGI KÖZPONT

A Nemzeti Kiberbiztonsági Központot [17] 2016. október 1-jén állították fel azzal a céllal, hogy az új kiberbiztonsági stratégiában lefektetett nemzeti ambíciók megvalósításának keretéül szolgáljon. A London központjában átadott új főhadiszállást hivatalosan 2017. február 14-én maga az angol uralkodó, II. Erzsébet királynő adta át. [18]

A Központ a GCHQ részeként működik, és azzal a céllal állították fel, hogy az országra leselkedő kiberfenyegetéseket csökkentse és az esetleges bekövetkezett támadások esetén hatékony válaszlépéseket tudjon tenni. Ebben szorosan együttműködik más brit szervezetekkel, vállalatokkal és magánszemélyekkel. Három létező kiberbiztonsági szervezetet fog össze és ezáltal helyettesít: a Kiberértékelési Központot (CCA), a CERT-UK-t és a CESG-et, és magába olvasztja a CPNI felelősségi körébe tartozó feladatokat is. Tevékenységét a nyitottság szellemében egyrészt a honlapján – melynek látogatottsága eléri a havi 100.000-et – keresztül is nyomon lehet követni: az első egy év alatt 51 jelentést és 37 iránymutatást készített a központ; másrészt a szervezet saját Twitter fiókkal is rendelkezik, amelyen egy év alatt 2000 bejegyzést tettek közzé a britek. A kormányzat és a vállalkozási szféra között az NCSC közvetítésével létrejött kezdeményezés, a Kiberbiztonsági Információmegosztási Partnerség[17] (CiSP) központi szerepet játszik a mintegy 30 különböző szektor érdekeinek kormányzat felé történő becsatornázásban.[18] Ehhez az NCSC a rendszeresen közzétett iránymutatásai és tanácsai révén járul hozzá.

A Központ az egyéves működése alatt elért eredményeiről a 2017. október 3-án kiadott *első éves értékelésben* ad számot. [19] Az elért eredmények között szerepel többek között az, hogy 1131 kiberincidenssel kapcsolatos bejelentést tártak fel, melyek közül 590 esetet súlyosnak értékeltek, 30 pedig olyan összetett eset volt, amely megoldása összkormányzati megközelítést igényelt. Ez utóbbi körbe tartozik például a 2017. májusi, a brit egészségügyi rendszert ért kibertámadás, amely során a hackerek 300.000 számítógépet fertőztek meg [20] vagy a 2017. június 25-én a brit Parlamentet ért támadás [21], amely eredményeképp 90, gyenge jelszóval védett levelezőfiókhoz és az ott tárolt adatokhoz fértek hozzá a behatolók – köztük a miniszterelnök asszony, Theresa May e-mail fiókjához is.[19]

A Központ kiemelt programja az *Aktív Kibervédelem* (Active Cyber Defence). Ennek keretében több száz kibertámadást sikerült kivédeni az elmúlt egy év alatt és az adathalászó oldalak átlagos online jelenlétét is sikerült leredukálni 27 óráról 1 órára. A program részeként négy szolgáltatást indított útjára a központ 2017 júniusában:

- a hamis e-mailek blokkolása: mintegy 120.000 ilyen jellegű támadást védtek ki, amelyek a gov.uk fiókok ellen irányultak;
- a kormányzati rendszerek fertőzött holnapokra történő átirányításának megakadályozása;
- a holnapokon felmerülő problémák gyors és hatékony orvoslása, amely valamennyi, a közszférában működő szervezet számára elérhető, és a konfigurációk beállításához, valamint adott rendszer sérülékenységének felméréséhez nyújt segítséget (ez

[17] Cyber Security Information Sharing Partnership
[18] A CiSP résztvevői köre egy év alatt 43%-kal növekedett és a platformot havonta több mint 4000-en látogatják.
[19] A legfrissebb jelentések szerint nem orosz, hanem iráni hackerek követték el a támadást. [22]

különösen a nem használt vagy nem frissített honlapok esetében jelenthet segítséget a támadókkal szemben);
- „rossz dolgok" internetről való eltávolítása: amennyiben adott szervezet érzékeli, hogy kéretlen e-maileket kap vagy felmerül annak lehetősége, hogy adathalászat áldozatává válhat, ezt jelzi a Netcraft magánvállalat felé, amely az adott honlappal szemben megteszi a szükséges figyelmeztető lépéseket.

A Központ tevékenységében a gazdasági és szociális szektor támogatása kiemelt helyen szerepel.[20] Mivel ezen szervezetek jelentős része kívül esik a közszférán, ezért speciális felkészítés szükségeltetik számukra. Ennek jegyében összeállították azt az iránymutatást, amely olyan egyszerű és minimális költséggel járó lépéseket tartalmaz, amelyek megtétele esetén nagymértékben csökkenthető adott vállalkozás kibertámadásnak való kitettsége.

A Központ tevékenységi körén belül kiemelt helyen szerepel a kiberszaktudás és gyakorlat feltételeinek kiépítése. Az tanulást nem lehet elég korán kezdeni – tartja a régi mondás, s ez nincs másképp a brit kiberoktatás helyzetét illetően sem. A *CyberFirst* elnevezésű programot azért hozták létre, hogy a fiatalok körében megszerettessék ezt a területet.[21] Eddig 20 vállalatot sikerült bevonni, de számuk folyamatosan növekszik. A programok között szerepelnek például a 2017 nyarán megszervezett kiberkurzusok, amelyeken a 14 és 17 év közötti korosztályból 1060 diák vett részt, de emellett évközben rendszeresen rendeznek alapszintű kurzusokat a fiatalok számára.[22] Kiemelt figyelmet fordítanak a lányok toborzására. 2017-ben a 13 és 15 éves lányok köréből 8000-en 2171 csapatot alkotva vettek részt az első, lányok számára kiírt kiberbiztonsági versenyen,[23] amely igen impozáns mutató és jól jelzi a kezdeményezés sikerét.[24] Egyetemi szinten is komoly befektetésekre került sor az elmúlt évben. 28 partnerszervezet 2,8 millió font értékben fektetett be a kiberképzés támogatásába 2017 márciusáig, valamint jelenleg már 14 Kiberbiztonsági Kiválósági Központ működik egyetemi keretek között, ahol a legmagasabb elméleti szinten járulnak hozzá e terület fejlődéséhez. Végezetül megemlítendő a CyberUK konferencia, amely háromnapos rendezvény minden évben egyesíti a terület szakembereit. Sikerét jól mutatja, hogy az idei konferencia résztvevői körében készített felmérés alapján jövőre a résztvevők 99%-a ismét részt kíván venni az eseményen.

A vállalati kiberkultúra kiépítése céljából útjára indított *Cyber Essentials* programról[25] a tanulmány első része már röviden említést tett, ezért ezen a ponton csak annyit emelek ki, hogy a program keretében eddig 7900 tanúsítványt állítottak ki, amely igazolja, hogy adott vállalat a biztonsági intézkedések minimum szintjét a vállalati kultúra integráns részévé tette. A másik, a

[20] A gazdasági szektor vonatkozásában ennek indokát az adja, hogy az online kereskedelem évente 10-15%-kal növekszik, és ezzel párhuzamosan az elkövetett csalások és más kiberbűncselekmények száma is drasztikusan növekszik.

[21] A nagyobb vonzerőt anyagi ösztönzőkkel is igyekeznek elősegíteni. Egyetemi hallgatóként évente 4000 font adómentes ösztöndíjat juttatnak a programban részt vevőknek, nyári diákmunka esetén heti 250 fontot fizetnek, a diploma megszerzését követően pedig garantálják, hogy három évig a kormányzati szférában e területen foglalkoztatják a programban részt vevőket. [23]

[22] A CyberFirst Defenders kurzus a 14-15 éves korosztály számára kiírt egynapos ingyenes kurzus. A CyberFirst Futures a 15-16 éves korosztálynak rendezett 5 napos ingyenes kurzus, emeltebb szinten. A CyberFirst Advanced kurzus, amely ötnapos ingyenes képzést biztosít, képezi a legmagasabb szintet, és ennek célközönsége szintén a 15-16 éves korosztály.

[23] CyberFirst Girls Competition

[24] A győztes a Lancaster Leányiskola „Körkörös logika" (Circular Logic) elnevezésű háromfős csapata lett.

[25] A kormányzati program olyan alapvető biztonsági intézkedések megtételét követeli meg a vállalatoktól, amelyek segítségével számítógépes rendszereik nagyobb biztonságban lesznek, így csökken annak esélye, hogy internetes bűnözés áldozatává válnak.

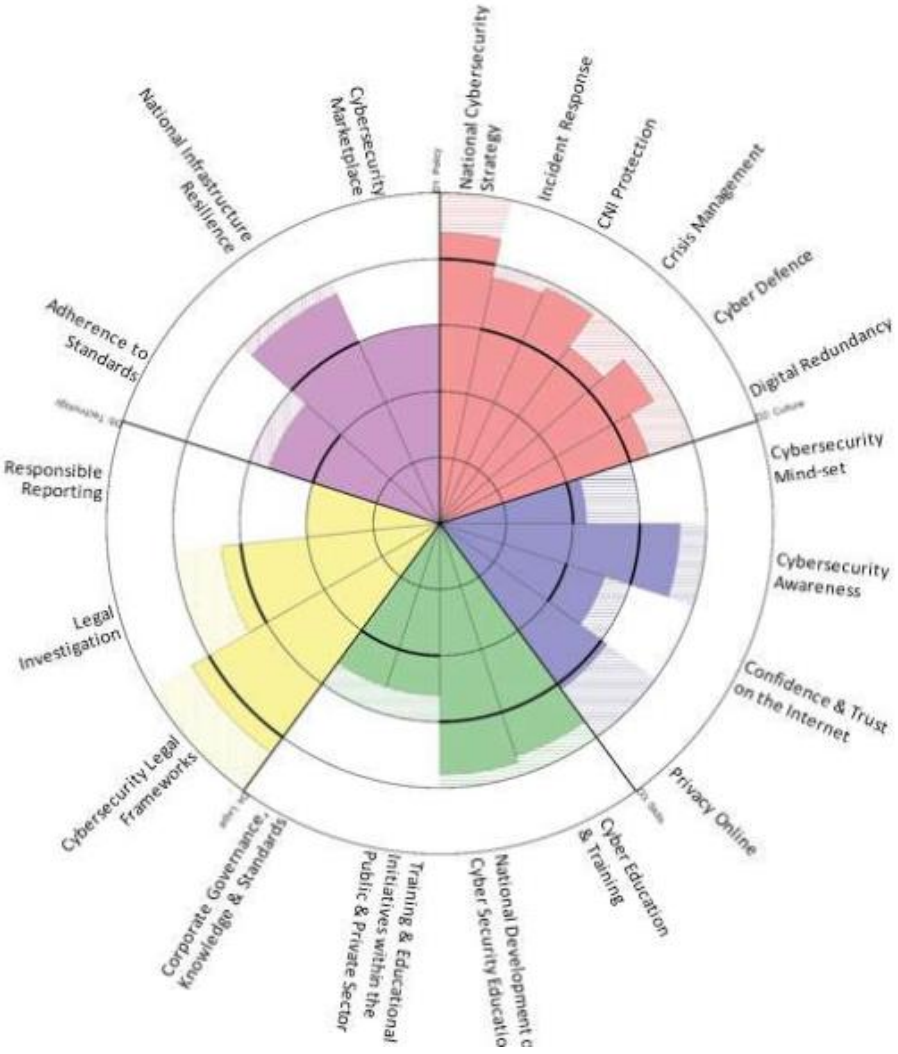
vállalati szektort érintő előremutató kezdeményezés az *Industry 100* elnevezésű program, amelyet az NCSC hivatalos megnyitó eseményén Philip Hammond kancellár indított útjára 2017. február 14-én. [24] A program keretében a vállalkozói és tudományos szféra elemzői, hálózatbiztonsági specialistái és az akadémiai szférában dolgozó szakemberek köréből szeretnének speciális szakértelemmel rendelkező alkalmazottakat toborozni a Központ állományába. [25]

A BRIT KAPACITÁSOK ÉRTÉKELÉSE

A brit kormányzat felkérésére a Globális Kiberbiztonsági Kapacitásközpont[26] (GCSCC) részletesen felmérte a jelenlegi brit kiberbiztonsági helyzetet, amely alapján kimutathatóak azok a területek, ahol további kormányzati intézkedések és stratégiai szintű befektetések szükségesek. A felmérés elkészítésében a központ segítségére voltak a minisztériumok, a tudományos élet, a törvényhozás, a magánszektor, a telekommunikációs nagyvállalatok, a pénzügyi szektor és a rendőrségi szervek is, akik egy négynapos konferencia keretében ütköztették álláspontjaikat. Nemcsak kerekasztal beszélgetésekre került sor, hanem meghatározott szempontrendszer szerint összeállított kérdőívek kitöltésére is.

A központ az elkészült jelentését 2016 novemberében publikálta. [26] Az értékelés elkészítésénél öt meghatározó szempontot vettek figyelembe: a politikaformálás és stratégiaalkotás; a kultúra és társadalom; az oktatás, képzés és szakképzettség; a jogi és szabályozási keretek; és a standardok, szervezetek és technológiák témaköreit. Mindegyik dimenzió esetében több tényezőt vizsgáltak meg, amelyek alapján végül adott területen felmutatott kiberkapacitást egy ötfokozatú skálán értékelték: kezdetleges fázisban lévőnek (start-up), formálódónak (formative), kiépítettnek (established), stratégiainak (strategic) vagy dinamikusnak (dynamic). Az Egyesült Királyság összesített értékelése a harmadik (kiépített) és a negyedik (stratégiai) fokozat között helyezkedik el, azonban a szórás meglehetősen nagy. Míg egyes területeken, mint például a stratégiaalkotás vagy a jogi keretek kialakítása (lásd infokommunikációs törvénykezés) terén kiemelkedően magas, dinamikus értékelést kapott az ország, addig a kiberkultúra dimenziójában a legjobb mutató is csak a kiépített szinten éri el. Ez utóbbi oka egyrészt az, hogy még mindig nem épült bele a gondolkodásmódba a tudatos internethasználat szükségessége – bár ez sajnos világszinten is problémát jelent –, másrészt pedig az internetbe vetett bizalom alacsony szintje. Az 1. sz. ábra mutatja az öt értékelés szemponton belül elért eredményeket.

[26] Global Cyber Security Capacity Centre



1. ábra Az Egyesült Királyság kiberkapacitása az öt vizsgált területen. [26]

Összességében tehát elmondható, hogy az Egyesült Királyság kiberkapacitásai már jelenleg is megfelelőek, de mindenképpen jó alapot nyújtanak a továbblépéshez. A további fejlődés előfeltétele azonban mindenképpen a megfelelő szakmai háttér, amely elengedhetetlen megfelelő szaktudással rendelkező munkaerő nélkül. Az ország azonban már jelenleg is súlyos szakemberhiánnyal küzd,[27] s ennek orvoslása – a stratégiában is rögzített becslés alapján – csak közel húsz év távlatában várható. [28] Felmérések szerint [29] a brit vállalatok 46%-a véli úgy, hogy a kiberszakember-hiányt a megrendelőik is megérzik, és ugyanilyen arányban gondolják úgy, hogy a probléma miatt kibertámadásoknak való kitettségük is nagyobb. A brit vállalatok 46%-a tervezi, hogy egy éven belül legalább 12%-kal megnöveli a kiber területen foglalkoztatott munkavállalói számát. Ugyanakkor a vállalatok nem nyitottak a friss diplomások fogadására: mindössze 6%-uk mutat erre hajlandóságot. Ennek következménye, hogy a fiatal kibermunkavállalók számaránya igen alacsony: a 35 év alatti korosztály mindössze 12%-ot tesz ki, ugyanakkor a 45 év felett korosztály 53%-ot. Tehát a kiberterületen dolgozó

[27] A kiberszakemberek hiánya világszintű probléma, és előrejelzések szerint 2022-re 1,8 millió szakember fog hiányozni a globális kiberbiztonsági piacról. [27] Megjegyzendő, hogy az előrejelzések 2020-ra a szakemberhiányt 1,5 millió főben jelölik meg, tehát két év alatt 20%-os növekedés várható ezen a területen. A tendencia tehát nem adhat okot bizakodásra.

szakemberek többsége egyre közelebb kerül a nyugdíjkorhatárhoz, ezért mihamarabb megfelelő megoldást kellene találni a pótlásukra.

KÖVETKEZTETÉSEK

Összességében megállapítható, hogy az Egyesült Királyság minden fronton igyekszik a lehető legkomplexebb módon felkészülni az esetleges kibertámadásokra: a stratégiaalkotástól kezdve a kormányzati intézkedéseken át egészen a vállalati szintű programokig. Azonban egyik ország sem lehet képes 100%-os felkészültségi szintet elérni, ezért támadások áldozataivá vál(hat)nak, ki kisebb, ki nagyobb mértékben. Ez a probléma az Egyesült Királyságot is érinti, és leglátványosabban akkor jelenik meg, amikor állami-kormányzati rendszereket ér támadás. Becslések szerint a kiberbűnözés által okozott éves kár mértéke 1 és 27 milliárd font között mozog, amely a brit gazdaságra is komoly kihatással lehet. [30]

A *brit kritikus infrastruktúra intézményei* ellen elkövetett támadások száma évről évre nő – ezt igazolják a fent említett 2017. évi események is. [31] Számos, a kritikus infrastruktúrához tartozó számítógépes rendszer esetében az jelenti a sérülékenység okát, hogy azokat még azelőtt terveztek, hogy a kiberbiztonsági kérdések ilyen mértéket öltöttek volna, illetve más, újabb rendszerek esetében pedig elmaradnak a szükséges biztonsági frissítések. [32] Az ilyen rendszerek ellen elkövetett kibertámadások hátterében megbúvó motivációk között említhető az anyagi haszonszerzés (például a zsarolóvírusokkal elkövetett támadások esetében), a közvélemény manipulálása, a támadó erejének demonstrálása, az információszerzés vagy a fizikai károkozás. Ugyanakkor elgondolkodtató az az adat, miszerint a nagy adatlopások 35%-ának hátterében emberi hanyagság, nemtörődömség vagy az alkalmazott rosszindulata áll. [33] Ezek olyan tényezők, amelyek viszonylag kis ráfordítással kiküszöbölhetőek lennének bármely szervezet esetében.

Jelenleg a brit kritikus infrastruktúra védelme az elsőszámú prioritások között szerepel. Ezt olyan intézkedésekkel kívánják elősegíteni, mint a tudományos és ipari kutatások ösztönzése, további titkosszolgálati és rendőrségi kapacitások kiépítése, a lakossági felkészültség fokozása és a szabályozás további cizellálása. Ha mindez a 2016-2021. közötti periódusban megvalósul, akkor a brit kiberkapacitások valamennyi mérőszám vonatkozásában kiváló értékelést kaphatnak, amely hűen tükrözi majd az ország tényleges felkészültségét és kapacitásainak meglétét, amelyek segítségével képes lehet szinte bármilyen jellegű, méretű, intenzitású és szándékú kibertámadás kivédésére – sőt akár támadó jellegű kiberműveletek végzésére is, ami deklaráltan is szándékában áll.

FELHASZNÁLT IRODALOM

[1] *Digital Landscape Research.* United Kingdom Cabinet Office, 2012. november 6. https://www.gov.uk/government/publications/digital-landscape-research/digital-landscape-research (letöltés ideje: 2017. október 11.)

[2] *Modernising Government 1999.* United Kingdom Cabinet Office, 1999. március. http://webarchive.nationalarchives.gov.uk/20131205101137/http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm (letöltés ideje: 2017. október 11.)

[3] *Digital Service Standard.* United Kingdom Cabinet Office https://www.gov.uk/service-manual/service-standard (letöltés ideje: 2017. október 11.).

[4] *Government Service Design Manual,* United Kingdom Cabinet Office, 2014. április https://www.gov.uk/service-manual (letöltés ideje: 2017. október 11.)

[5] *European Union Digital Agenda Scoreboard.* https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/indicators#ebusiness (letöltés ideje: 2017. október 11.)

[6] OSULA, Anna-Maria: *National Cyber Security Organization: United Kingdom.* CCDCOE, Tallinn, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf (letöltés ideje: 2017. október 11.)

[7] National Security Secretariat https://www.gov.uk/government/organisations/national-security/about (letöltés ideje: 2017. október 11.)

[8] *Office of Cyber Security & Information Assurance – OCSIA* https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance (letöltés ideje: 2017. október 11.)

[9] MOLNÁR D.: *Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia.* In: Hadmérnök XII. évfolyam 3. szám, 2017.

[10] Government Communications Headquarters (GCHQ) https://www.gchq.gov.uk/ (letöltés ideje: 2017. október 11.)

[11] *Defence Secretary Announces Ł40m Cyber Security Operations Centre.* 2016. április 1. https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre (letöltés ideje: 2017. október 11.)

[12] *Defence and Cyber Security: Goverment response to the Committee's Sixth Report of Session 2012-13.* United Kingdom House of Commons Defence Committee, 2013. március 22. https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm (letöltés ideje: 2017. október 11.)

[13] *Defence Cyber Operations Group:* Finance: Written question - 26326. United Kingdom Ministry of Defence, 2016. február 8., http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-02-08/26326/ (letöltés ideje: 2017. október 11.)

[14] *New cyber reserve unit created* 2013. szeptember 29. https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (letöltés ideje: 2017. október 11.)

[15] *Working for JFC.* https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment (letöltés ideje: 2017. október 11.)

[16] *Global Operations and Security Control Centre (GOSCC).* Defence Committee, Further written evidence from the Ministry of Defence. 2013. március 12. https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106we05.htm (letöltés ideje: 2017. október 11.)

[17] *National Cyber Security Centre (NCSC)* https://www.ncsc.gov.uk/ (letöltés ideje: 2017. október 11.)

[18] *Her Majesty the Queen opening the new National Cyber Security Centre.* 2017. február 15. https://www.gchq.gov.uk/her-majesty-queen-opening-new-national-cyber-security-centre (letöltés ideje: 2017. október 11.)

[19] *The 2017 Annual Review*, National Cyber Security Centre, 2017. október 3., https://www.ncsc.gov.uk/news/2017-annual-review (letöltés ideje: 2017. október 11.)

[20] *NHS seeks to recover from global cyber-attack as security concerns resurface.* 2017. május 13. https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack (letöltés ideje: 2017. október 11.)

[21] *Cyber-attack on UK parliament: Russia is suspected culprit.* 2017. június 25. https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit (letöltés ideje: 2017. október 11.)

[22] *Iran blamed for cyber attack on Parliament that hit dozens of MPs, including Theresa May.* 2017. október 14., http://www.telegraph.co.uk/news/2017/10/13/iran-responsible-cyberattack-british-parliament/ (letöltés ideje: 2017. október 14.)

[23] *CyberFirst* https://www.gchq-careers.co.uk/early-careers/cyberfirst.html (letöltés ideje: 2017. október 11.)

[24] *Chancellor's speach at the National Cyber Security Centre opening.* 2017. február 14. https://www.ncsc.gov.uk/news/chancellors-speech-national-cyber-security-centre-opening (letöltés ideje: 2017. október 11.)

[25] *Industry 100 Initiative* https://www.ncsc.gov.uk/industry-100 (letöltés ideje: 2017. október 11.)

[26] *Cybersecurity Capacity Review of the United Kingdom.* Global Cyber Security Capacity Centre, University of Oxford, 2016. november, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf (letöltés ideje: 2017. október 11.)

[27] *Cyber-Workforce Shortage to Increase to 1.8 Million Positions by 2022.* 2017. február 15. https://www.infosecurity-magazine.com/news/cyberworkforce-shortage-to/ (letöltés ideje: 2017. október 11.)

[28] *National Cyber Security Strategy 2016-2021*. HM Government, United Kingdom, 2016. november 1., https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (letöltés ideje: 2017. október 11.)

[29] *Global shortfall of cyber security workers to reach 1.8 million in 5 years.* 2017. február 15. http://www.information-age.com/demand-cyber-security-skills-increasing-123464166/ (letöltés ideje: 2017. október 11.)

[30] *The cost of cybercrime.* A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office. 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf (letöltés ideje: 2017. október 11.)

Over Ł1bn lost by businesses to online crime in a year. 2016. június 13. http://www.actionfraud.police.uk/news/over-1bn-lost-by-businesses-to-online-crime-in-a-year-jun16 (letöltés ideje: 2017. október 11.)

[31] Annual Report 2015/2016, CERT_UK. https://www.ncsc.gov.uk/content/files/protected_files/report_files/CERT-UK-Annual-Report-2015-16.pdf (letöltés ideje: 2017. október 11.)

[32] *Cyber Security of UK Infrastructure.* Houses of Parliament, Postnote no. 554, 2017. május researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf (letöltés ideje: 2017. október 11.)

[33] *Building a Cyberresilient Organization.* The Boston Consulting Group, 2017. https://www.bcgperspectives.com/Images/BCG-Building-a-Cyberresilient-Organization-Jan-2017_tcm80-218439.pdf (letöltés ideje: 2017. október 11.)