Várady Eszter – Kelemen Gábor

Kibervédelmi tanúsítási rendszerek és egy egységes uniós kibervédelmi rendszerrel kapcsolatos vállalati attitűdök

A Századvég primer kutatásának összefoglalója

1. Bevezetés

A digitalizáció, az innovatív technológiák megjelenése és megállíthatatlan terjedése gyökeresen alakítja át a lakosság, a vállalkozások és a közigazgatás mindennapi működését, munkafolyamatait. Ennek a fundamentális változásnak az origójában az IKT-szektor és az ott tevékenykedő vállalkozások állnak.

Tekintve, hogy a digitális megoldásokkal szembeni bizalom közvetve egy ország nemzetgazdaságát és versenyképességét is érdemben befolyásolja, illetve hiánya vagy elvesztése egy ország fejlődését is visszavetheti, kiemelt nemzetgazdasági érdek, hogy az IKT-szektor által előállított eszközök és szolgáltatások a felhasználói bizalom megtartása és megerősítése érdekében megfelelő biztonságot nyújtsanak.

A digitális megoldások biztonsági szintjét Európa-szerte számos biztonsági tanúsítási rendszer értékeli, ugyanakkor egységes, uniós szintű tanúsítási rendszer egyelőre eddig még nem jött létre. Ezt a helyzetet kezelendő az Európai Bizottság már dolgozik egy ilyen kiberbiztonsági tanúsítási keretrendszer kidolgozásán, amelynek bevezetése vélhetően minden európai uniós tagállamban kötelező lenne, ami új helyzet elé állíthatja a hazai IKT-szektorban tevékenykedő vállalkozásokat is.

Fentiek okán a Századvég Konjunktúrakutató Zrt. Digitális Üzletága az Innovációs és Technológiai Minisztérium megbízásából kvantitatív és kvalitatív eszközökkel kutatást végzett az IKT-szektor vállalkozásai körében. A kutatás azt vizsgálta, hogy az érintett magyar piaci szereplők miként viszonyulnak az uniós szabályozási törekvésekhez, hogyan fogad-

nának egy egységes, minden érintettre kiterjedő szabályrendszert, illetve az milyen hatást gyakorolna a mindennapi működésükre, az általuk előállított termékekre/megoldásokra.

1.1. A kutatás indíttatása

A digitális eszközöket és szolgáltatásokat fejlesztő és forgalmazó vállalkozások számos biztonsági megoldást kínálnak ügyfeleik számára az eszközhöz, szolgáltatáshoz való fizikai hozzáférés korlátozásától a távoli illegális hozzáférés elleni védelmen át a vírusok, spamek és malware-ek elleni védelemig. Ezek biztonságossá tétele az irántuk való bizalom fontos feltétele, ennek hiánya pedig súlyosan korlátozza e technológiák elterjedését.

Mivel a digitalizáció az innováció, s ezzel a gazdasági fejlődés egyik motorja, a digitális megoldásokkal szembeni bizalom hozzájárul egy ország innovációs potenciáljának növekedéséhez is, míg annak hiánya a közigazgatással és az általa nyújtott elektronikus szolgáltatásokkal szembeni bizalmat is alááshatja (például a személyes adatok megfelelő védelmére vonatkozó garanciák hiányában).

Az IKT-szektor növekedési potenciálját tehát érdemben befolyásolja az, hogy a felhasználók bíznak-e a szóban forgó termékekben, szolgáltatásokban, és ez különösen fontos egy olyan országban, mint Magyarország, ahol az IKT-szektor nemzetgazdaságban betöltött szerepe uniós összehasonlításban is jelentősnek mondható. Az Eurostat[1] adatai szerint 2019-ben az IKT-szektor a teljes GDP 6,1 százalékát adta, ami egyértelműen az átlagon felül teljesítő országok közé sorolja Magyarországot. Hasonló eredményt mutatnak a KSH 2020-ra vonatkozó számai is, amelyek nem a GDP-hez, hanem a bruttó hozzáadott értékhez (GVA) viszonyítják a szektor teljesítményét, és amelyek szerint 2020-ban a szektor a teljes hazai GVA 7,2 százalékát adta.[2] 2020-ban összesen 234,4 ezer embernek biztosított munkát közvetlenül, ami a nemzetgazdaságban foglalkoztatottak 5,3 százalékát jelentette abban az évben. Az IKT-szektor két alágazatába tartozó regisztrált és működő vállalkozások száma 2020-ban meghaladta az 52 ezret (ez az összes működő vállalkozás valamivel több mint 6 százaléka). Mennyiségi értelemben az IKT-szektorba sorolt vállalkozások több mint 97 százalékát az IKT-szolgáltatást nyújtók ad-

[1] https://ec.europa.eu/eurostat/databrowser/view/tin00074/default/table?lang=en

[2] Az eltérést egyrészt az egyes évek között bekövetkezett fejlődés, másrészt a GDP és a GVA eltérő tartalma okozza. A GDP már tartalmazza a termékadók és terméktámogatások egyenlegét is, míg a GVA nem.

ták, ugyanakkor a kibocsátásból, hozzáadott értékből és foglalkoztatásból való részesedésük aránya jóval kisebb. Mindkét alkategóriában látványos a (különösen az 1–4 főt foglalkoztató) mikrovállalkozások dominanciája: az IKT-feldolgozóiparban működő vállalkozások több mint 72, az IKT-szolgáltató szektorban tevékenykedőknek pedig több mint 91 százaléka ebbe a létszám-kategóriába esik. 250 fő felett mindössze nyolcvan vállalkozást találunk, de az összes IKT-cégen belüli több mint 97 százalékos súllyal szemben itt csak kétharmadot tesznek ki az IKT-szolgáltató cégek.

1. táblázat: A hazai IKT-szektor elemei a TEÁOR '08 besorolás szerint

IKT-feldolgozóipar („C": feldolgozóipar nemzetgazdasági ág)	IKT-szolgáltatás („J": információ, kommunikáció nemzetgazdasági ág)
C.26: Számítógép, elektronikai optikai termék gyártása	
C.26.1: Elektronikai alkatrész, áramköri kártya gyártása	J.58: Kiadói tevékenység
C.26.2: Számítógép, perifériás egység gyártása	J.59: Film-, videógyártás, televízióműsor gyártása, hangfelvétel-kiadás
C.26.3: Híradástechnikai berendezés gyártása	J.60: Műsor-összeállítás, műsorszolgáltatás
C.26.4: Elektronikus fogyasztási cikk gyártása	J.61: Távközlés
C.26.5: Műszer-, óragyártás	J.62: Információtechnológiai szolgáltatás
C.26.6: Elektronikus orvosi berendezés gyártása	J.63: Információs szolgáltatás
C.26.7: Optikai eszköz gyártása	
C.26.8: Mágneses, optikai információhordozó gyártása	

FORRÁS: KSH, SZÁZADVÉG-SZERKESZTÉS

Az Európa-szerte működő számos biztonsági tanúsítási rendszer mellett egységes, uniós szintű tanúsítási rendszer egyelőre nem jött létre, az Európai Bizottság a 2019-ben elfogadott ún. Cybersecurity Act alapján dolgozik egy ilyen keretrendszeren, ami az EB véleménye szerint minden érintett szereplő számára egyszerűbb és egyértelműbb helyzetet teremtene. Egy ilyen rendszer nem megfelelően előkészített és/vagy túlságosan erőltetett ütemű bevezetése és alkalmazásának kötelezővé tétele versenyhátrányba hozhatja a hazai IKT-szektor kevésbé tőkeerős szereplőit a korlátlan erőforrásokkal rendelkező piacvezető globális szereplőkkel szemben.

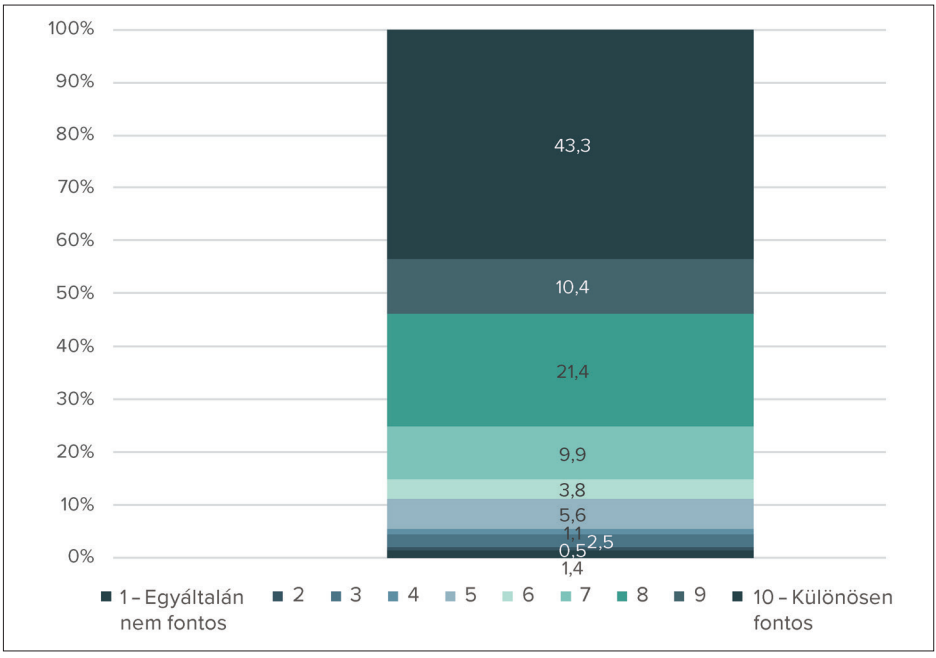
2. A primer kutatások eredményeinek összefoglalása

2.1. A kvantitatív felmérés eredményei

A Századvég Digitális Gazdaságfejlesztési Üzletága több mint 440 hazai IKT-vállalkozás és több szakértő megkérdezésével kutatást végzett annak felmérésére, hogy a hazai IKT-cégek mennyire ismerik és alkalmazzák termékeik, szolgáltatásaik előállítása során a kiberbiztonsági megoldásokat,

illetve hogyan fogadnák egy uniós szintű keretrendszer bevezetését. Alapvetően fontosnak tartják a kiberbiztonsági kérdéseket: 88,8 százalékuk fontosnak (6 és 10 pont közötti értékelés a tízes skálán), a cégek háromnegyede nagyon fontosnak (8 és 10 pont közötti érték), ezen belül 43,3 százalék kiemelten fontosnak (10 pontos értékelés) tartja. További 5,6 százalék közepesen fontosnak (5 pont) tekinti a témát, és mindössze minden huszadik cég tartja kevéssé lényegesnek ezt a területet (1 és 4 közötti pontérték).

1. ábra: Értékelje egy 1-től 10-ig terjedő skálán, hogy az Önök vállalkozása számára mennyire fontosak a kiberbiztonsági kérdések, milyen hangsúlyt helyeznek erre a témára? (A megkérdezettek %-ában, n = 443)



FORRÁS: SZÁZADVÉG-SZERKESZTÉS

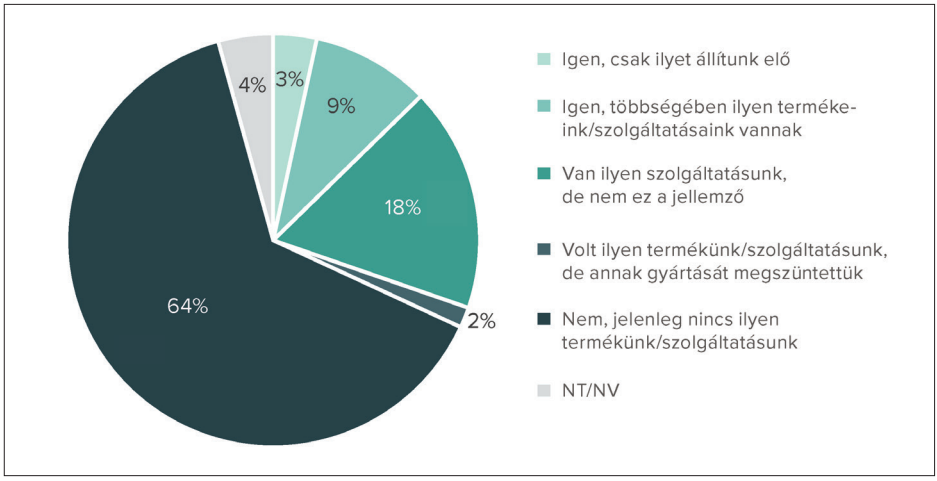
A kutatásból az derült ki, hogy kiberbiztonsági tanúsítványt a megkérdezett IKT-cégek mintegy harmada használ saját termékei, szolgáltatásai minősítésére, jellemzően a megrendelői elvárásoknak való megfelelés miatt, illetve az iparági sztenderdekhez való igazodás érdekében.

A kibervédelmi tanúsítványok, illetve kibervédelmi megfelelőségértékelési rendszerek alkalmazása az interjúk keretében megfogalmazott szakértői becslésekhez képest némiképp magasabb a felmérésbe bevont

hazai IKT-vállalkozások körében: 30,3 százalékuk jelenleg is használ valamilyen kiberbiztonsági tanúsítványt saját termékei, illetve szolgáltatásai minősítésére. Közülük minden tizedik vállalkozás kizárólag (3 százalék), minden harmadik (9 százalék) pedig többségében kibervédelmi tanúsítvánnyal értékelhető terméket vagy szolgáltatást állít elő. A többségüknél azonban nem az ilyen termékek, szolgáltatások a meghatározóak: a vállalkozások kétharmada jelenleg nem használ ilyen megoldásokat, mert vagy nincs releváns terméke, szolgáltatása, vagy megszüntette már az ilyen termék gyártását (2 százalék).

A jelenség hátterében az a lehetséges magyarázat áll, hogy a megkérdezett vállalkozásoknak az az 51,5 százaléka, amelynek szüksége van ilyen típusú megoldásokra, nem kizárólag a saját gyártású termékek, szolgáltatások auditálására használja, hanem vagy a termékek, szolgáltatások előállítása vagy például a cég mindennapi működése (vállalatirányítási rendszer, hálózati eszközök, központi IT-infrastruktúra stb.) során alkalmazza.

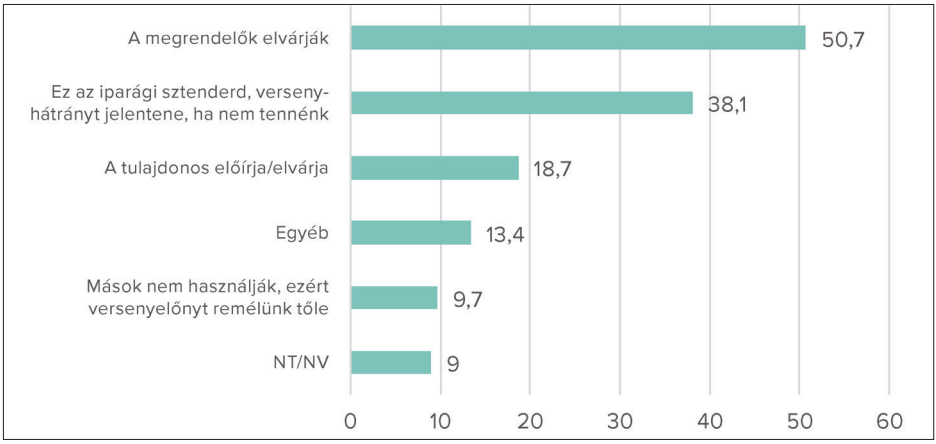
2. ábra: Az Önök vállalkozása állít-e elő olyan terméket/szolgáltatást, amelynek kiberbiztonsági megfelelősége értékelhető és igazolható tanúsítvánnyal? (A megkérdezettek %-ában, n = 443)



FORRÁS: SZÁZADVÉG-SZERKESZTÉS

A kiberbiztonsági tanúsítvány használatát leginkább a megrendelők elvárásai, illetve az iparági sztenderdekhez való igazodás motiválja: a 134 vállalkozás fele (50,7 százalék) az előbbi, 38,1 százaléka pedig az utóbbi miatt. A tulajdonosi elvárás miatt alkalmazott tanúsítványok aránya csekélyebb (18,7 százalék).

3. ábra: Miért alkalmaznak kiberbiztonsági tanúsítványokat az érintett termékek vagy szolgáltatások értékelésére? (A kiberbiztonsági tanúsítvánnyal ellátható termékeket és szolgáltatásokat előállítók %-ában, n = 134)



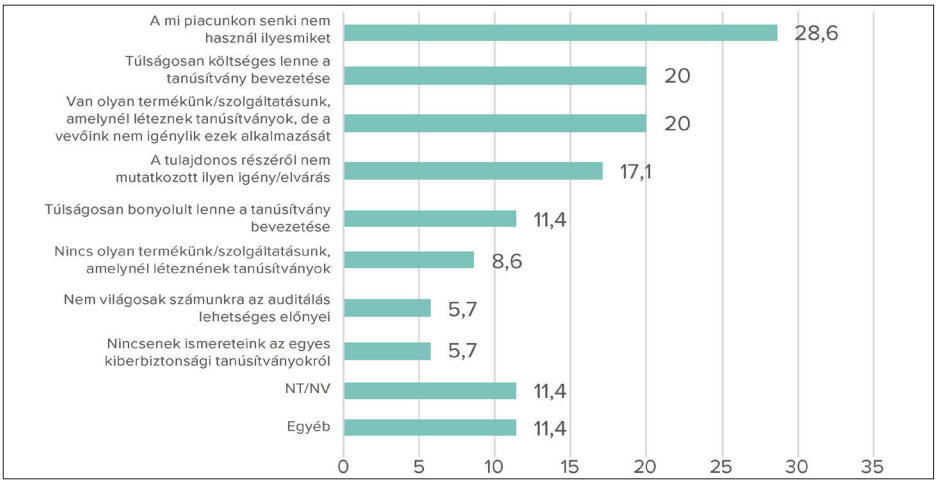
FORRÁS: SZÁZADVÉG-SZERKESZTÉS

Kutatásunk során azt is felmértük, milyen okokra vezethető vissza, hogy az IKT-vállalkozások, melyek állítanak ugyan elő kibervédelmi tanúsítvánnyal értékelhető termékeket vagy szolgáltatásokat, mégsem teszik. Legjellemzőbben az iparági gyakorlat, a vevői és tulajdonosi elvárások hiánya, valamint a tanúsítási eljárással járó magas költségek képeznek akadályt. A használat ellen szól továbbá, hogy a bevezetés költségessége és erőforrásigénye miatt jelenleg nem feltétlenül jelent rövid távon üzleti előnyt a vállalatok számára. Az ilyen megoldásoktól való távolmaradást a megkérdezettek emellett az egységes tanúsítási rendszer, illetve a megrendelői és tulajdonosi elvárások hiányával indokolták. A kiberbiztonsági tanúsítványok elterjedését a megkérdezett vállalkozások szerint elsősorban az erre vonatkozó megrendelői elvárások erősödése, az e célra elérhető támogatások rendelkezésre állása és/vagy a jogszabályi kötelezés gyorsíthatná fel.

Egy esetleges uniós szintű, egységes kibervédelmi tanúsítási rendszer bevezetésének a kiberbiztonsági tanúsítással értékelhető termékeket és szolgáltatásokat előállító vállalkozások 38,8 százaléka örülne, mert az várakozása szerint hozzájárulna a piac átláthatóbbá válásához. További 44 százalék nem örülne ugyan, de alávetné magát a döntésnek, és eleget tenne a jogszabályi előírásoknak. Minden huszadik érintett cég (5,2 százalék) megfontolná a kötelező tanúsítvánnyal érintett termék gyártásának beszüntetését ilyen fejlemény esetén, 0,7 százalékuk pedig kategorikusan kijelentette, hogy kivonulna a piacról. A válaszadók mai tudása szerint tanúsítványt igénylő termékkel, szolgáltatással nem rendelkező cégeket

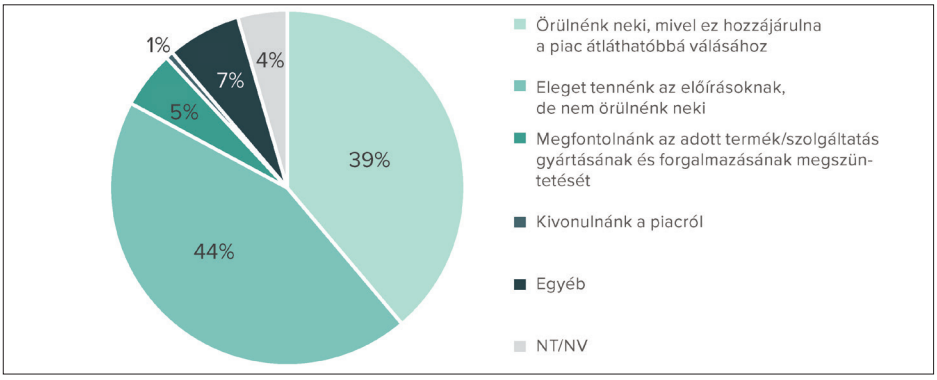
az egységes tanúsítási rendszer fogadtatásáról nem kérdeztük, mivel válaszaik relevanciáját nehéz volna megítélni.

4. ábra: Ha az Önök vállalkozása nem használ kiberbiztonsági tanúsítványokat, akkor ez milyen okokra vezethető vissza? (Azok körében, akik állítanak elő kibervédelmi tanúsítvánnyal értékelhető termékeket, szolgáltatásokat, de mégsem látják el azokat tanúsítvánnyal, a megkérdezettek %-ában, n = 35)



FORRÁS: SZÁZADVÉG-SZERKESZTÉS

5. ábra: Hogyan reagálnának Önök arra, ha a termékeik/szolgáltatásaik valamelyikét akár európai uniós, akár hazai jogszabályi előírás alapján kötelezően kiberbiztonsági tanúsítvánnyal kellene ellátni? (A kiberbiztonsági tanúsítvánnyal ellátható termékeket és szolgáltatásokat előállítók %-ában, n = 134)

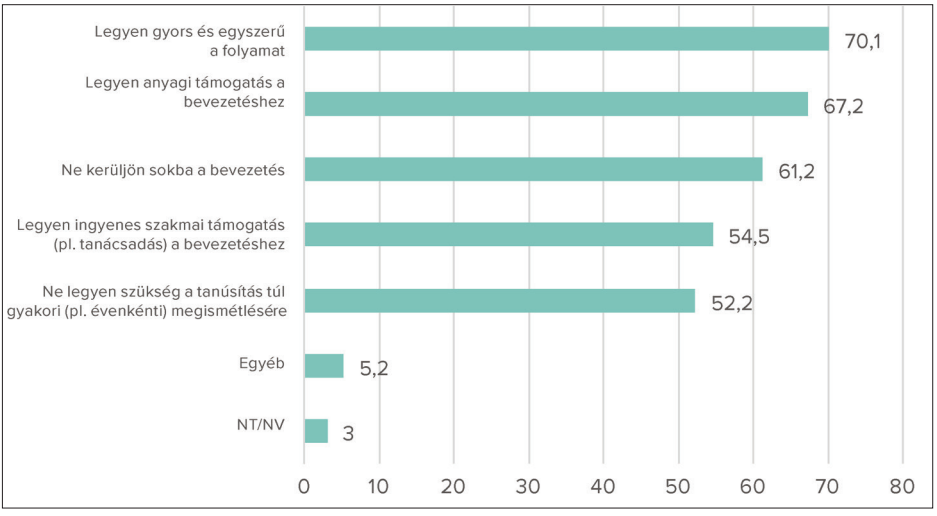


FORRÁS: SZÁZADVÉG-SZERKESZTÉS

Az egységes rendszer bevezetése a megkérdezett szakértők szerint rövid távon minden bizonnyal szűkítené a piaci kínálatot, ugyanakkor emelné az érintett termékek, szolgáltatások minőségét és megbízhatóságát, nemzetközi szinten is versenyállóbbá téve őket – akár új piacokat is megnyitva előttük. Továbbá piactisztító hatása is lenne, mivel kikopnának az európai piacról az olcsó, de nem biztonságos termékek, illetve azok a vállalkozások, amelyek nem tudnak és/vagy nem akarnak megfelelni egy ilyen kötelezettségnek.

Egy esetleges uniós szinten kötelező, egységes kiberbiztonsági értékelési folyamat bevezetésétől a válaszadók elsősorban a folyamat gyorsaságát és egyszerűségét várják el (70,1 százalék). Emellett a bevezetéssel járó anyagi terhek alacsony szintje (61,2 százalék), illetve a bevezetéshez kapható anyagi támogatás (67,2 százalék) is az elvárásaik között szerepel. Az ingyenes szakmai tanácsadást a válaszadók több mint fele (54,5 százalék) említette, de többségben (52,2 százalék) vannak azok is, akik szerint „ne legyen szükség a tanúsítás túl gyakori megújítására". Az önálló válaszok között többen is említették, hogy a már meglévő tanúsítások integrálása az egységes uniós rendszerbe kiemelt fontosságú volna a tanúsítványokat már használók körében.

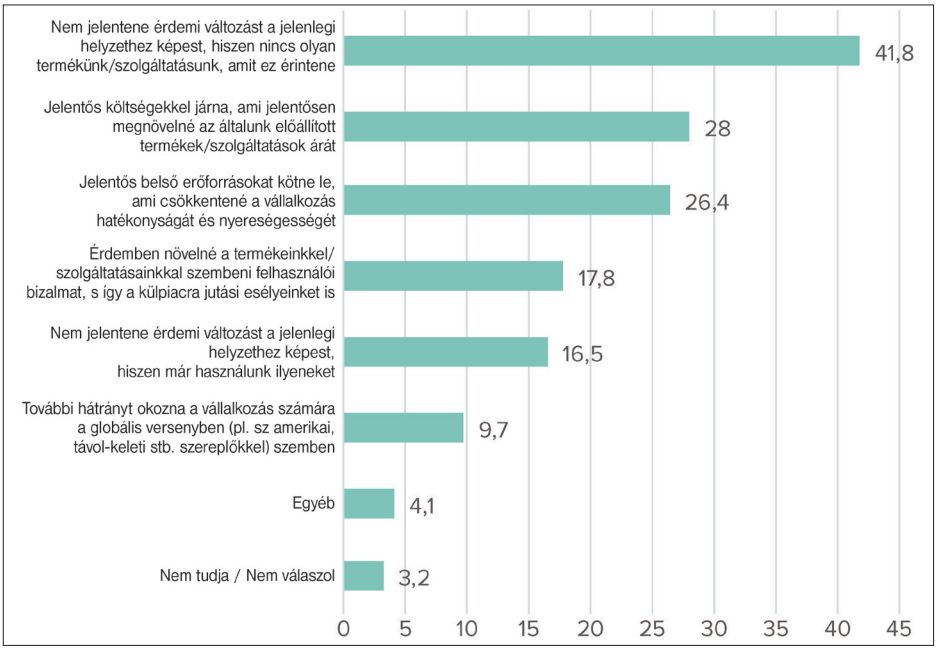
6. ábra: Ha kötelezővé válna valamely termékükre/szolgáltatásukra a kiberbiztonsági tanúsítvány, akkor milyen elvárásokat támasztana egy ilyen értékelési folyamattal szemben? (A kiberbiztonsági tanúsítvánnyal ellátható termékeket és szolgáltatásokat előállítók %-ában, n = 134)



FORRÁS: SZÁZADVÉG-SZERKESZTÉS

Az egységes uniós rendszer vállalati működésre gyakorolt hatását a teljes mintán kérdeztük le, mivel ez azokat a cégeket is érinti, amelyek a tanúsítványok felhasználói, ha saját maguk nem is rendelkeznek tanúsítást igénylő termékkel vagy szolgáltatással. A hazai IKT-vállalkozások több mint felének (58,3 százalék) nem befolyásolná a mindennapi működését. Ennek oka, hogy nincs érintett terméke vagy szolgáltatása (41,8 százalék), vagy már most is használ valamilyen kibervédelmi tanúsítványt. További 28 százalék vélekedik úgy, hogy a tanúsítási rendszer bevezetése jelentős költségekkel járna a szektor szereplői számára, ami tovagyűrűző hatásként az IKT-szektor által előállított termékek és szolgáltatások árát is emelné. A megkérdezettek több mint negyede (26,4 százalék) tart attól, hogy jelentős belső erőforrásokat emésztene fel a tanúsítási rendszer bevezetése, ami csökkentené a vállalkozás hatékonyságát és nyereségességét. Az IKT-vállalkozások alig 10 százaléka nyilatkozta azt, hogy további versenyhátrányt jelentene számára az egységes rendszer bevezetése a globális versenytársakkal szemben (amerikai, távol-keleti stb. szereplők).

7. ábra: Hogyan befolyásolná az Önök vállalkozásának működését a kiberbiztonsági tanúsítványok rendszerének kötelezővé tétele (Az összes megkérdezett %-ban, n = 443)



FORRÁS: SZÁZADVÉG-SZERKESZTÉS

2.2. A kvalitatív felmérés eredményei

A kibervédelmi szakértőkkel folytatott interjúk alapján öt olyan szempont rajzolódott ki, melyek motiválhatják a hazai vállalkozásokat a tanúsítványok használatára: versenyelőny megszerzése, megrendelői vagy vásárlói elvárásoknak való megfelelés, tulajdonosi elvárások teljesítése, jogszabályi előírásoknak való megfelelés, pályázati, illetve ágazati előírások kielégítése.

Több interjúalanyunk is megjegyezte, hogy a tanúsítások használata jelenleg nem feltétlenül jelent előnyt a vállalatok számára, ezek ugyanis rendkívül erőforrás-igényes folyamatok, költségeik érthető módon a termékek és szolgáltatások árában jelennek meg, amelyek jellemzően drágábbak a nem tanúsított (adott esetben harmadik országból importált) megoldásoknál. A magyar piacra jellemző árérzékenység miatt jelenleg akár versenyhátrányba is kerülhetnek a tanúsított termékek és szolgáltatások a tanúsítvánnyal nem rendelkező konkurenciával szemben.

Egy vállalkozásnak alapvetően akkor származik előnye a tanúsításból, ha nem a hazai, hanem az európai vagy a globális piacra szállít. Ebben az esetben viszont a tanúsítás megléte nem versenyelőnyt jelent, hanem a piacra lépés egyik alapfeltétele. A magyar IKT-szereplők a globális környezetben csak akkor érvényesülhetnek, ha van a piac által elvárt tanúsításuk. Egy nemzetközileg elfogadott keretrendszernek való megfelelés előírása előrelépést jelentene a hazai piacon, hiszen ezek a keretrendszerek általában tágabb elvárásokat fogalmaznak meg, gyakorlatiasabbak, ugyanakkor széles körben elfogadottak. Nemzetközi (de legalább európai szintű) tanúsítvány birtokában jóval nagyobb piac felé nyithatnának a hazai vállalkozások.

2. táblázat: A kibervédelmi tanúsítások használata, illetve nem használata mögött meghúzódó megfontolások a hazai vállalkozások körében – szakértői vélemények alapján

	Tanúsítvány használata	Tanúsítvány nem használata
Előnyök	• minőségi garancia (termék/szolgáltatás biztonsági kompromittálásának garantált elkerülése) • nemzetközi/globális piacra lépés feltétele	• a termék/szolgáltatás ára alacsonyabb marad a tanúsítvánnyal szemben • csak rövid távon jelenthet előnyt
Hátrányok	• versenyhátrány a hazai piacon: drágább termék (az ár maghatározóbb a biztonsággal szemben) • drága befektetés • lassú megtérülés • hosszú távon viszont a tanúsítással rendelkező megoldásoké lesz a jövő	• rendkívül szigorúan ellenőrzött piacra lépés akadályozott (egyáltalán nem jellemző) • versenyhátrány: iparági sztenderd elvárás esetén • támadás esetén ügyfélbizalom és ügyfélvesztés kockázata áll fenn

FORRÁS: SZÁZADVÉG-SZERKESZTÉS

Az egységesen bevezetett, kötelező tanúsítási rendszer a szakértők egybehangzó véleménye szerint rövid távon biztosan szűkítené a kínálatot, ugyanakkor piactisztító és konszolidációs hatása is jelentős lenne. Közép- és hosszú távon ugyanakkor számítani lehetne a tanúsítvánnyal ellátott megoldások kínálati piacának bővülésére. Az egységes biztonsági rendszernek köszönhetően a kínálati oldal minősége mindenképpen növekedne, összességében maga a kibertér válhatna biztonságosabbá, ami pedig a fogyasztói oldalon a legfontosabb eredmény.

Nemzetközi összehasonlításban a magyar termékek és szolgáltatások versenyképesebbé, versenyállóbbá válhatnának. A keresleti oldal jelentős változására ugyanakkor nem kell számítani, egy egységes, minden érintett szereplőre nézve kötelező tanúsítvány bevezetését követően nyilván csak a tanúsítással rendelkező termékek és szolgáltatások maradhatnának piacon (konszolidációs hatás).

Jelenleg a magyar cégek árazásában jellemzően nem vagy minimális mértékben jelenik meg a kiberbiztonság, illetve az ezzel kapcsolatos fejlesztések költsége. Ha megjelenik a kényszer (egy egységes tanúsítási rendszer bevezetésével), az a költségekben is szemmel láthatóvá válik. Ennek ellentételezésére többen is javasolták az ilyen típusú fejlesztések költségeinek esetleges állami támogatását. A szakértői vélemények ebben a kérdéskörben konszenzust mutattak: a megkérdezett interjúalanyok rövid távon a tanúsítvánnyal ellátott termékek és szolgáltatások árának 5-10 százalékos növekedésére számítanak, ugyanakkor ezt egyszeri hatásnak tartják; a későbbiekben az árat alapvetően a piaci folyamatok alakítanák organikusan.

Az európai (és a magyar) piacon jelenleg hatalmas mennyiségű importált (elsősorban kínai, amerikai, dél-koreai) IKT-termék érhető el. Egy egységes rendszer bevezetésével a harmadik országból származó eszközök is ellenőrizhetővé válnának az EU piacán, ami európai termékek számára versenyelőnyt is hozhatna, hiszen az európai gyártók átállását minden bizonnyal támogatná valamilyen formában a kormányuk. Az evolúciós folyamat végén a valódi nyertesek a felhasználók lennének, akik garantáltan jobb minőséget kapnának.

Az interjúk során elhangzott válaszokból egyértelmű, hogy a szakértők mindenképpen javasolják állami ösztönző rendszer kialakítását, amennyiben sor kerül egy egységes európai tanúsítási rendszer bevezetésére, mert enélkül nem lenne jó a rendszer fogadtatása a piaci szereplők között, ezért fontos lenne a bevezetéshez valamilyen kormányzati segítséget nyújtani.

A primer kérdőíves és szakértői mélyinterjús kutatásokból levont következtetések alapján az uniós keretszabályozástól függetlenül is szükség volna a hazai IKT-vállalkozások kiberbiztonsággal és kiberbiztonsági tanúsítványokkal kapcsolatos tudatosságának, ismereteinek és attitűdjeinek fejlesztésére a tanúsítással rendelkező hazai termékek és szolgáltatások körének bővítése érdekében. Ahhoz, hogy a hazai cégek az egységes rendszer esetleges bevezetésének a nyerteseivé, és ne elszenvedőivé váljanak, kutatásunk szerint az alábbi feltételek megteremtésére volna szükség: biztonságos fejlesztési kultúra kialakítása (edukáció a vállalkozások körében); társadalmasítás és edukáció; támogató jogszabályi környezet megteremtése; a bevezetés szakmai és anyagi támogatása; a fokozatosság garantálása, tesztidőszakok és állami ajánlások bevezetésével; a bevezetés egyszerűsége, az indokolatlanul gyakori megújítás mellőzése; oktatási rendszer fejlesztése; egyéb ösztönzők (például versenyelőny biztosítása, közbeszerzési elvárások módosítása).

3. Összefoglalás

Kiberbiztonsági tanúsítványt a megkérdezett IKT-cégek mintegy harmada használ saját termékei, szolgáltatásai minősítésére, jellemzően a megrendelői vagy tulajdonosi elvárásoknak való megfelelés miatt, illetve az iparági sztenderdekhez való igazodás érdekében. A használat ellen szól, hogy a bevezetés költségessége és erőforrásigénye miatt jelenleg nem feltétlenül jelent rövid távon üzleti előnyt a vállalatok számára. Az ilyen megoldásoktól való távolmaradást a megkérdezettek emellett az egységes tanúsítási rendszer, illetve a megrendelői és tulajdonosi elvárások hiányával indokolták.

A kiberbiztonsági tanúsítványok elterjedését a megkérdezett vállalkozások szerint elsősorban az erre vonatkozó megrendelői elvárások erősödése, az e célra elérhető támogatások rendelkezésre állása és/vagy a jogszabályi kötelezés gyorsíthatná fel. Egy esetleges uniós szintű, egységes kibervédelmi tanúsítási rendszer bevezetésének az érintett vállalkozások 38,8 százaléka örülne, mert az várakozásaik szerint hozzájárulna a piac átláthatóbbá válásához; további 44 százalék nem örülne ugyan, de alávetné magát a jogszabályi előírásoknak.

Az egységes kiberbiztonsági tanúsítási rendszer bevezetése a megkérdezett szakértők szerint rövid távon minden bizonnyal szűkítené a piaci kínálatot, ugyanakkor emelné az érintett termékek, szolgáltatások minőségét és megbízhatóságát, nemzetközi szinten is versenyállóbbá téve őket – akár új piacokat is megnyitva előttük, illetve piactisztító hatása is lenne.

Irodalom

Common Criteria (CC). https://www.commoncriteriaportal.org/

Common Criteria Recognition Arrangement (CCRA) 2014: Megállapodás a közös kritériumok tanúsítványainak elismeréséről az információtechnológiai biztonság területén. https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

Európai Bizottság 2019a: Az EU kiberbiztonsági törvénye. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Európai Bizottság 2019b: Az uniós kiberbiztonsági tanúsítási keretrendszer. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

Eurostat 2022: Az IKT-ágazat GDP-hez viszonyított aránya. https://ec.europa.eu/eurostat/databrowser/view/tin00074/default/table?lang=en

KSH TEÁOR '08-kódok. https://www.ksh.hu/teaor_kereso

National Institute of Standards and Technology (NIST). https://www.nist.gov/cyberframework/framework

NIST 800-53. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ISO 15408. https://www.iso.org/standard/50341.html

ISO 17420-1. https://www.iso.org/standard/74979.html

ISO 27000. https://www.iso.org/isoiec-27001-information-security.html

ISO 9000. https://www.iso.org/iso-9001-quality-management.html

ETSI EN 303645. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Szabályozott Tevékenységek Felügyeleti Hatósága. https://sztfh.hu/tevekenysegek/kiberbiztonsag-felugyelete/