Brehel József

Kiberbiztonság – az információs társadalmi környezet kockázatai

Kiberbiztonsági helyzetkép, kockázatelemzés és kockázatértékelés.

1. Bevezetés, hazai és Európai helyzetkép

A hazai és az európai kiberbiztonsági helyzetkép összefoglaló ismertetése érdekében néhány idézettel kezdem, amelyek az elektronikus, illetve írott sajtóban jelentek meg a témában. Egy előadás is ide kívánkozik a teljesség érdekében:

„Rajnai Zoltán, Magyarország kiberkoordinátora előadást tartott – Velem vagy mellettem? címmel a ITBN budapesti IT- és Kiberbiztonsági konferencián. „

Az előadás alcíme: „A magyarországi kormányzati kiberkoordináció helyzete, az állami és piaci szereplők együttműködésének formái”[14] volt.

Ennek kapcsán fogalmazódott meg néhány gondolat és készültek innovációs lehetőséget is tartalmazó javaslatok, melyeket a hazai kibervédelmi körképet követően ismertetünk.

IDÉZETEK:

„Kezdjük mindjárt a jó hírrel:

Az elmúlt időszakban nem történt nagy veszteséget okozó kár a kormányzati hálózatokban. – mondta még az előadása elején Rajnai Zoltán, Magyarország kiberkoordinátora..”

Megjegyzés: Ez persze nem jelenti azt, hogy nem is történik ilyen a jövőben.

KÉRDÉS: Felkészültünk-e erre? És ha igen akkor milyen mértékben?

Az ezt biztosító magyar kibervédelem gyakorlati oldala éppen egy évvel ezelőtt alakult át és vette fel a mai formáját, középpontban a Nemzeti Kibervédelmi Intézettel.

2. HAZAI HELYZETKÉP

2.1 „Egy kézben a magyar kibervédelem[9]

„Központosított a kormányzat, de ez egyáltalán nem biztos, hogy jó. Van olyan eset, amikor több hivatal helyett nem biztos, hogy jobb a kevesebb, a kibervédelem összetett kérdése pont ilyen lehet. A NATO jelentése[9] egyelőre csak bemutatja az új helyzetet." Rajnai erről ezúttal nem beszélt, inkább a jogalkotói oldalt mutatta be.

A lényeg röviden: 2013-ban a parlament elfogadta a Nemzeti Kiberbiztonsági Stratégiát.[10]

Ugyanebben az évben megszületett a ma is érvényben lévő infótörvény[11] ennek a stratégiának a megvalósítására.

A kormány egy rendelettel[12] létrehozta a Nemzeti Kiberbiztonsági Koordinációs Tanácsot és a Kiberbiztonsági Fórumot, hogy ezt a törvényt konkrét feladatokra bontsák és azokat végre is hajtsák. Olajozottan hangzik, igaz? A gyakorlatban persze ennél kicsit döcögősebb a történet:

2.2 A kormány biztonságot akar, a cégek eladni?

A tanácsnak viszont csak tanácsadási, javaslattételi jogköre van, még hat munkacsoportostól is. Konkrét technikai tanácsot nem adnak, hiszen;

Miniszterek, államtitkárok, valljuk be őszintén, talán a legkevesebbet fognak érteni ahhoz, hogy technikailag milyen megoldásokat lehet alkalmazni.

Ezért hozta létre az a bizonyos kormányrendelet a tanács mellett a Kibervédelmi Fórumot is. Itt keresik a technikai megoldásokat a problémákra, de itt már nem a kormányzati oldal, hanem a magánszektor, a szakma tesz javaslatokat a konkrét technikai megvalósításokra. A kiberkoordinátor, vagyis most Rajnai feladata pedig éppen a két oldal: a politikai és a piaci szereplők közötti közvetítés. Ha önnek ez kicsit lassúnak hangzik, akkor nem egyedül gondolja ezt, hanem Rajnai Zoltánnal együtt:

„Már most elkéstünk, amikor a legújabb kibervédelmi módszereket kell a támadások ellen kidolgozni” – mondta a kiberkoordinátor.

Rajnai szerint a vállalati szféra elsősorban abban érdekelt, hogy legyen minél könnyebben használható, így minél eladhatóbb ez a védelem, vagyis a hozzáférés az elektronikus adatokhoz. "Sajnos néha a cégek szándékosan gyengítik azt az információbiztonsági szintet, ami jogszabályi oldalról elvárt lenne" – mondta a cégek képviselői előtt állva. Két éve épp az ITBN zárásaként hangzott el, hogy ha nem történik valami nagy változás,

„Magyarország a személyes adatai kétharmadát nem fogja tudni megvédeni.

Minden 4 adatból 3 felfedésre, eltulajdonításra kerül.”

Újabb pontban érthetünk egyet a kiberkoordinátorral, ha ön is azt gondolja, hogy ez óriási probléma. Rajnai szerint ha nem tudjuk megvédeni az adatainkat, úgy járhatunk, mint az Egyesült Államok, ahol tavaly sok millió társadalombiztosítási adatot tudtak ellopni a hekkerek. De említhette volna éppen a több amerikai állam választói adatbázisa elleni támadásokat is, amelyekből legalább az egyik bevallottan sikeres volt. Abba most ne is gondoljunk bele, hogy mi lenne velünk, ha a magyar adatokat övezné olyan érdeklődés, mint az amerikaiakat.

2.3 Az ITBN CONF EXPO 2016

A konferencián Rajnai beszélt még arról is, hogy szintén nagyon fontos a kritikus infrastruktúrák kibervédelme. Ezt elsősorban az Országos Katasztrófavédelmi Főigazgatóság látja el, de a kiberkoordinátor szerint nem szabad magára hagyni ebben a katasztrófavédelmet, mert ott nincs meg az a szakmai tudás, ami önmagában elég lenne a szükséges védelem biztosításához.

Szintén fontos még az információmegosztás, ami Rajnai szerint az amerikai kibervédelem első számú pillére, itthon viszont még van hova előre lépni ebben. Kell is hova, hiszen a hálózati és információs rendszerek biztonságáról szóló NIS-irányelvet a közelmúltban fogadta el az Európai Unió, és ennek az elemeit 2018-ig át kell ültetni a hazai kibervédelembe is.

3. EURÓPAI HELYZETKÉP

3.1 Európa felkészül a kiberháborúra

„Életbe lépett az első uniós kiberbiztonsági szabályozás. Ideje volt, mert egyre több a veszély. Itthon egész jól állunk, de azért van még teendő.”

Ezzel az idézettel még találkozni fogunk.

Az Európai Unió már évek óta dolgozik azon, hogy megerősítse a kontinens kiberbiztonságát. Van is miért, évről évre egyre több a fenyegetés, egyre gyakoribbak a támadások. A személyes adataink védelmére hozott közelmúltbeli rendelet után most újabb kirakósdarab, a legfontosabb európai szolgáltatások védelmére hivatott NIS-irányelv is hatályba lép. Az EU-ra jellemző komótos tempóban, de lassan összeáll a 21. századhoz igazított kibervédelem. Na és Magyarországra milyen feladatok várnak?

Miközben a társadalmunk egyre elképzelhetetlenebb internet vagy mobileszközök nélkül, és a gazdaság is egyre nagyobb részben támaszkodik digitális infrastruktúrákra, ez a rengeteg pozitívummal járó átalakulás egyben beláthatatlan biztonsági kockázatot is hozott.

3.2 A hekkerek, akik 17 millió forintot kerestek több százmillió jelszón

Ez viszont csak az az összeg, amit az adatok eladásából szereztek. Valószínűleg évekig saját célra használták ezeket, és jó eséllyel az ön jelszava is a neten kering. Lépésről lépésre bemutatjuk, hogyan védheti meg magát.

Szinte hetente derül fény újabb és újabb durva adatlopásokra, azt pedig mi magunk is teszteltük, hogy még a privát wifihálózatok sincsenek biztonságban. Az utóbbi években viszont az egy-egy céget vagy a felhasználók adatait érintő veszélyek mellett megszaporodtak a kritikus infrastruktúra elleni támadások is. 2007-ben például Észtországot érte átfogó kibertámadás, a kórházakat sorban fertőzik meg a zsarolóvírusok, és tavaly történt az ukrán elektromos hálózat addig példátlan meghekkelése is. Oroszországgal szemben pedig gyakorlatilag jelenleg is folyik a kiberháború.

3.3. Javában zajlik a kiberháború Oroszországgal

Az észak-európai országok nem csak az online hadviseléstől tartanak, az információs hadviselésben pedig a V4-ek is célpontok.

A példákat persze lehetne még sorolni: egy felmérés szerint 2015-ben 38 százalékkal több kiberbiztonsági incidenst jelentettek globálisan, mint egy évvel korábban. Ezért egyre nagyobb szükség van összehangolt stratégiára és a gyakorlatban is hasznos szabályozásra. Már csak azért is indokolt a közös EU-s fellépés, mert nemcsak a szolgáltatások nyúlnak át ma már rutinszerűen az országhatárokon, de egy-egy hálózat- vagy információbiztonsági incidens is kihathat az egész Unióra.

3.4 Az EU kiterjeszti a biztonságot. Ennek egyik pillére a GDPR

Ebben a helyzetben nem csoda, hogy az EU a maga bürokratikus megfontoltságával, de sorban fogadja el a biztonságosabb digitális mindennapok megteremtésére hivatott szabályozásokat. Korábban leginkább csak a távközlési és az internetszolgáltatók voltak kénytelenek foglalkozni a kiberbiztonsággal, mert csak rájuk vonatkoztak az EU által 2012-ben bevezetett hálózatbiztonsági, adatvédelmi és incidens bejelentési kötelezettségek. Az új szabályozások egyik célja éppen ennek a kiterjesztése a távközlési piacon túlra is.

Az EU új információbiztonsági rendje két fő pillérre épül. Az egyik a tagországok adatkezelését közös nevezőre hozó általános adatvédelmi rendelet, a **GDPR**. Ez az európai állampolgárok személyes adatait védi minden eddiginél alaposabban, és egységes működési keretet biztosít az ezeket az adatokat kezelő cégeknek.

3.5 Sosem látott szigor jön az adatvédelemben

Hatályba lépett az új EU-s adatvédelmi rendelet, amely nagyobb felhasználói kontrollt és egységes szabályozást ígér. De mi változik, hogyan és miként érinti ez a felhasználókat?

3.6 A második pillér a NIS

A másik pillér pedig az augusztus elején frissen életbe lépett, a hálózati és információs rendszerek biztonságáról szóló irányelv, vagyis a **NIS**. Ez az első uniós szintű kiberbiztonsági szabályozás, amely az EU szerint segíthet megelőzni az európai infrastruktúra elleni kibertámadásokat. Július 6-án hagyta jóvá az Európai Parlament (EP), és augusztus 8-án lép hatályba. Célja közös nevezőre hozni a tagállamok kibervédelmét, meghatározni egy közös biztonsági minimumot, és ehhez közös eszköztárat – intézményi rendszert, szabályozást – adni a kezükbe.

Az irányelv legfontosabb jellemzői dióhéjban:

- Két csoportra vonatkozik: az alapvető szolgáltatást nyújtó szolgáltatókra (vagyis a kritikus infrastruktúrára) és a digitális szolgáltatókra.
- Komolyabb biztonságot követel meg, és kötelező incidens bejelentést ír elő kibertámadások esetén.

- A tagállamoktól saját kiberstratégia és felügyeleti intézmények létrehozását várja el, illetve lefekteti a tagállamok közötti kötelező együttműködés kereteit.

4. Az európai infrastruktúra védelme

„A NIS nem általános szabályozás, hanem két konkrét csoportra vonatkozik, azokra, amelyeknek a megtámadása a legérzékenyebben érinti a társadalmat. Az egyik ilyen halmaz az alapvető szolgáltatást nyújtó szolgáltatóké: digitális infrastruktúrák, energiacégek, ivóvízellátók, közlekedési vállalatok, egészségügyi szolgáltatók, banki szolgáltatások, pénzügyi piaci infrastruktúrák tartoznak bele. Az ide sorolandók pontos körét a tagállamok maguk határozzák meg az alapján, hogy az adott szervezet szolgáltatása alapvető-e a társadalom vagy a gazdaság számára, ennek a szolgáltatásnak a biztosítása függ-e hálózati és információs rendszerektől, illetve egy kiberbiztonsági incidens jelentős zavart okozna-e a szolgáltatásban.”

"Ezeken az ágazatokon belül sem mindenre és mindenkire vonatkozik, hanem csak azokra a konkrét szolgáltatásokra, amelyeknek a kiesése komoly társadalmi vagy gazdasági károkat okozna. Ha egy kibertámadás nagyobb fennakadást okoz egy ország áramellátásában, az ide tartozik. Ha a támadás viszont csak az adott áramszolgáltató marketingrészlegét lövi le két-három napra, akkor nem biztos. Az első esetben ugyanis a kritikus infrastruktúra védelme és a lakosság alapvető áramellátása közvetlenül sérülnek, a másodikban viszont csak az adott szolgáltató szenved el némi üzleti kellemetlenséget." – magyarázta az Indexnek Précsényi Zoltán, aki a Symantec biztonsági cég brüsszeli kormányzati kapcsolati menedzsereként részt vett az új szabályozások előkészítésében.

A másik érintett csoportba azok a digitális szolgáltatásokat nyújtó szolgáltatók tartoznak, amelyek ugyan nem nélkülözhetetlen, de fontos társadalmi hatású szolgáltatásokat kínálnak: az online piacterek, a keresőszolgáltatások és a felhőszolgáltatók. (Az irányelv korábbi tervezetében a közösségi oldalak is szerepeltek, de a végleges változatból kikerültek – vagyis kimondatott, hogy Facebook nélkül is van élet.) Fontos, hogy azokra a szolgáltatókra is vonatkozik a NIS, amelyek az EU-n kívüliek, de itt is szolgáltatnak, tehát például az amerikai Amazonra vagy Google-re. Ugyanígy, a brexit ellenére a brit cégeknek is meg kell felelniük az irányelvnek, ha az EU-n belül működni akarnak.

4.1 Nagyobb szigor, kötelező jelentések

Nagyobb a szigor, náluk a tagállamok hatóságai ellenőrizhetik, hogy milyen biztonsági lépéseket terveznek, és hogy ezeket a gyakorlatba is megfelelően átültetik-e.
Jelentős átfedés van a két új szabályozás, a GDPR és NIS rendelkezései között, hiszen mindkettő meghatároz biztonsági előírásokat és incidens bejelentési kötelezettséget.

A két jogszabály két különböző aspektusból és két különböző cél érdekében támaszt egyébként eléggé hasonló elvárásokat.

Teljesen más irányból közelít viszont a két szabályozás, és más típusú incidensekre vonatkoznak:

- A GDPR célja a személyes adatok és a magánszféra védelme, ezért a központjában a felhasználó áll. A NIS-ben a hálózatvédelmen van a hangsúly, és a szolgáltatókra hegyezték ki.

- A GDPR minden cégre vonatkozik, amelyik európai állampolgárok személyes adatait kezeli, a NIS hatásköre jóval szűkebb, csak a legfontosabb szolgáltatásokra összpontosít.

- A GDPR szerint akkor kell bejelenteni egy biztonsági incidenst, ha személyes adat forog kockán, a NIS alatt akkor, ha az adott szolgáltatás kerül veszélybe.

- Ha személyes adat kompromittálódik, a GDPR értelmében az adott cég köteles az adat tulajdonosát, vagyis a felhasználót is értesíteni, a NIS hatálya alá tartozó cégeknek elég a felügyelő hatóságnak bejelentést tenni "jelentős hatású" hálózati incidens esetén.

Hogy mennyire számít jelentős hatásúnak egy biztonsági esemény, attól függ, hány embert érint a szolgáltatás-kimaradás, mennyi ideig tart, és földrajzilag mennyire kiterjedt; illetve a digitális szolgáltatók esetében még attól is, hogy milyen mértékű zavart okoz a szolgáltatásban, és mekkora hatást gyakorol az adott szolgáltatásra épülő gazdasági és társadalmi tevékenységekre. A tagállamoknak e szempontok szerint kell majd pontosan meghatározniuk a feltételeket, amikor átültetik az irányelvet a maguk nemzeti jogrendjébe.

Mindkét csoport számára két fontos változást hoz az irányelv. Egyrészt a kockázatokkal arányos mértékű hálózat- és rendszerbiztonságot kell garantálniuk, másrészt be kell jelenteniük az illetékes nemzeti hatóságnak, ha mégis valamilyen jelentős biztonsági incidens éri őket. Az alapvető szolgáltatások esetében viszont

4.2 Szorosabb európai együttműködés

„A kibertámadások gyakran egyszerre több tagállamot érintenek, a szétforgácsolt védelem sebezhetővé tesz minket.”

– mondta Andreas Schwab, az Európai Parlament illetékes jelentéstevője a NIS elfogadásakor, amelynek éppen az a fő célja, hogy szorosabbra fűzze az együttműködést. Ehhez a tagállamoknak több feladatuk is van az irányelv élesedéséig hátralévő 21 hónapos türelmi időben. A főbb feladatok:

- A NIS alapján ki kell dolgozniuk egy nemzeti hálózat- és információbiztonsági stratégiát.
- Ki kell jelölniük egy nemzeti hatóságot, amely felügyeli a NIS átültetését és végrehajtását.
- Ki kell jelölniük egy vagy több gyors reagálású kibervédelmi csapatot, ezek az úgynevezett CSIRT-ek (Computer Security Incident Response Team) vagy CERT-ek (Computer Emergency Response Team). (A kettő ma már szinonimának számít, az EU a CSIRT kifejezést használja, Magyarországon inkább a CERT-et preferálják a hatóságok.)
- Szektoronként meg kell határozni, pontosan milyen kritériumok alapján számít egy-egy cég az irányelv hatálya alá, és ezután a konkrét cégeket is ki kell jelölni. Erre a 21 hónapos átültetés után még további 6 hónapja lesz a hatóságnak.
- EU szinten pedig létre kell hozni a kiberbiztonsági csapatok együttműködését koordináló CSIRT-hálózat, illetve a nemzeti hatóságok együttműködését segítő Együttműködési Csoportot is. Mindkét szervezet felállítására fél éve van az EU-nak – vagyis a tagállamoknak közösen –, de érezhetően gyorsan akarnak haladni, ezért ezeket már el is kezdték előkészíteni.

A szabályozás részleteinek a kidolgozására az Európai Bizottság létrehozott egy szakértői csoportot még májusban. Ennek magyar részről a Nemzeti Kibervédelmi Intézet (NKI) a

tagja, és általában is az egész kiberbiztonsági szervezkedésben ők képviselnek minket, ezért őket kérdeztük arról, milyen feladatok állnak még Magyarország előtt, és mit várnak az új irányelvtől. Itt volt már az ideje

A GDPR-t 2018 májusától kezdik alkalmazni (közvetlenül, hiszen az egy rendelet), és a NIS-t is ugyaneddig kell átültetni a nemzeti jogrendekbe (mivel az csak irányelv). Vagyis alkalmazni a gyakorlatban.

5. 2018-ra áll össze az új európai kiberpáncélzat.

Annyi biztos, hogy már épp ideje is lesz, mert a kiberbiztonság gyorsan változó terület, az EU malmai viszont lassan őrölnek: a GDPR-t 2012-ben kezdték kidolgozni, a NIS első tervezete 2013-as, vagyis mire életbe lépnek, már 5-6 évesek lesznek.
"Az eredeti javaslatok évekkel ezelőtti beterjesztése óta végeláthatatlan viták zajlottak Brüsszelben arról, hogy azok életképesek, indokoltak, arányosak-e." – mondja Précsényi. Egyesek sokkal nagyobb szigort követeltek, mások már így is túlszabályozással riogattak. Viszont amikor tavaly decemberben már látszott, hogy milyen lesz a végleges változatuk, akkor a szakmán belül a vitát felváltotta a verseny: ki milyen gyorsan, milyen ügyesen lesz képes alkalmazkodni az új szabályokhoz, és milyen hatékonyan fog élni a bennük rejlő új lehetőségekkel. 2018-ig a legfontosabb itthoni tennivaló, hogy meg kell ismertetni az új szabályokat az érintett ágazatok szereplőivel, és együtt kidolgozni a megvalósítás részleteit. Ki kell jelölni a azokat a cégeket is, amelyekre konkrétan vonatkozni fognak itthon az új előírások. Mindeközben a részletek EU-s szintű kidolgozásában is részt kell venni: az Együttműködési Csoport beindításában, illetve az incidensek bejelentése pontos menetének meghatározásában.

6. A Kiberbiztonsági kockázatok elemzése és kezelése

6.1 Kiberbiztonsági állapotfelmérést és helyzetelemzést, kockázatelemzést és akcióterv kidolgozását támogató megoldás

IDÉZET: *„Életbe lépett az első uniós kiberbiztonsági szabályozás. Ideje volt, mert egyre több a veszély. Itthon egész jól állunk, de azért van még teendő.”*

Kezdjük ezzel az idézettel és ennek kapcsán gondoljuk végig, hogy hogy is és hol is állunk (merre haladunk) ma Magyarországon a kibervédelem, kiberbiztonság terén (hazai helyzetkép, helyzetfelmérés) és milyen teendőink vannak ebből a helyzetből adódóan, továbbá az EU-s jogszabályi megfelelés tekintetében az elkövetkezendő években.

Az idézet: - amely a sajtóban megjelent fenti „Európa felkészül a kiberháborúra” c. cikkből származik, még egyszer tehát:

„Életbe lépett az első uniós kiberbiztonsági szabályozás. Ideje volt, mert egyre több a veszély. Itthon egész jól állunk, de azért van még teendő.” Ennek kapcsán néhány kérdés és gondolat merül fel:

Mit is jelent pontosan az, hogy „egész jól állunk”? – mire alapozza ezt a kijelentést a tisztelt cikkíró? A mérnökben az alábbi kérdések merülnek fel:

Volt felmérés ebben a témában? Ha igen, milyen körben? Milyen módszertannal?

Ezek ismeretében és eredményeképpen kijelenthetjük-e, hogy egész jól állunk?

NEM HISZEM. EZ CSAK EGY BECSLÉS LEHET, AMI VAGY IGAZ, VAGY NEM. AZ ÁLLÍTÁST MILYEN SZÁMOKKAL ÉS TÉNYEKKEL - BIZONYÍTÉKOKKAL TUDJUK ALÁTÁMASZTANI?

ÉN ÚGY GONDOLOM, HOGY NEM TUDOM, NEM TUDJUK PONTOSAN, HOGY IS ÁLLUNK VALÓJÁBAN! DE MEGTUDHATJUK.

HOGYAN?

6.2 A javaslat:

VÉGEZZÜNK EGZAKT TUDOMÁNYOS ALAPOKON NYUGVÓ FELMÉRÉST, (ÖNÉRTÉKELÉST) ÉS AZ EREDMÉNYEK ÉRTÉKELÉSE, ELEMZÉSE ALAPJÁN ADJUNK PONTOS HELYZETKÉPET. EHHEZ A MÓDSZERTAN ÉS AZ ESZKÖZ IS ADOTT.

6.3 A módszertan és az eszköz:

A JAVASOLT FELMÉRÉSI ESZKÖZ: A NIST – (National Institute of Standards and Technology, továbbiakban: NIST) Cyber Security Excellence Builder Toolkit (Draft/Tervezet) dokumentuma. Ennek az eszköznek, mint papíralapú kérdőívnek a későbbiekben - várhatóan és vélhetően a jövő év, 2017 elején - új elektronikus verziója is lesz (Excel vagy egyéb program támogatás). Ezért célszerű az alábbi linken is megtalálható (CEBEREYE) Blog és/vagy a NIST Institute weblapok figyelemmel kísérése.

A cikk angol nyelvű linkje:

- **NIST offers cyber self-assessment tool, updates email security guidance**

A NIST kiadott egy biztonsági felmérést és értékelést támogató új eszközt, amely segítségével a szervezetek jobban megérthetik, felmérhetik, pontosabb ismeretek birtokába juthatnak saját kiberbiztonságuk és annak menedzselésével kapcsolatos helyzetük, erőfeszítéseik és előre haladásuk tekintetében.

A NIST által javasolt Kiberbiztonsági önértékelési eszköz (Tervezet, 2016 Szeptember)

Az eszköz elsősorban a versenyszféra képviselőire került kifejlesztésre, de értelemszerűen elvei és gyakorlata jól alkalmazhatók az állami, kormányzati szektorban is. Minél szélesebb a felmérés köre, annál pontosabb képet kaphatunk arról, hogyan is állunk valójában és melyek a teendőink a jövőben.

7. Kibervédelmi kiválóság fejlesztési és állapot felmérési eszköz (angol verzió, tervezet).

Baldrige Cybersecurity Excellence Builder

Key questions for improving your organization's cybersecurity performance
Draft September 2016

National Institute of Standards and Technology (www.nist.gov)

7.1 Az eszköz összefoglaló ismertetése

Az új eszköz - USA Nemzeti Szabványügyi és Technológiai Intézete (a NIST) szerint – az általuk bevezetett és alkalmazott folyamat segítségével a felhasználó szervezetek felmérhetik a Kiberbiztonsági helyzetüket, - Kiberbiztonsági karakterisztika és szükséges stratégiai lépések, valamint képesek lesznek az alábbiakra:

- **Meghatározhatók azok a kiberbiztonsággal kapcsolatos tevékenységek, amelyek fontosak az üzleti, ügymeneti stratégia és a kritikus szolgáltatások biztosítása szempontjából.**

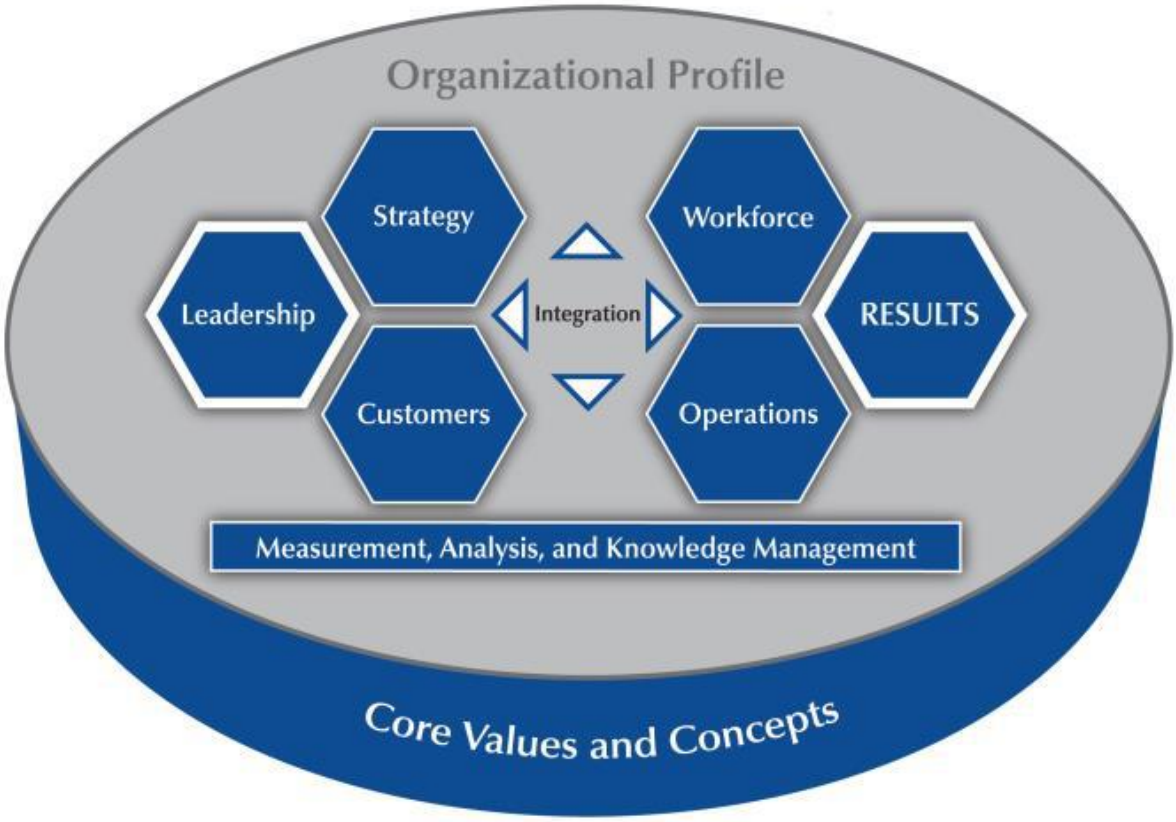
- **Priorizálhatók, rangsorolhatók a kiberbiztonsági kockázatkezelési intézkedések és kiadások, beruházások.**
- **Felmérhetők az alkalmazott kibervédelemmel kapcsolatos alkalmazott szabványok, irányelvek és gyakorlati megoldások hatékonysága és eredményessége.**
- **Felmérhetők a kiberbiztonsági eredmények**
- **Azonosíthatók és rangsorolhatók a szükséges továbbfejlesztések.**

A felmérés, önértékelés eredményeként az adott szervezet Fejlettségi/Érettségi besorolást kap – melynek szintjei lehetnek: reaktív/reagáló, korai, fejlett, vagy szerep alapú modell – és ennek ismeretében minden szervezet kidolgozhatja saját fejlesztési intézkedési tervét és megalapozott döntéseket hozhat a kiberbiztonság javítása, szükséges szintjének emelése érdekében. **Fentiek miatt javasoljuk és tekintjük a tanulmány fő tárgyának az említett eszközt.**

A továbbiakban az alkalmazással, az eszköz használatának módjával, a kérdésekkel és a várható gyakorlati eredményekkel foglalkozunk.

7.1.1 Az (ön-)értékelés elemei és folyamata

Szervezeti profil és kontextus – (Az 1. sz. ábra: A „Baldrige Excellence Framework” alapján)



1. sz. ábra: A szervezeti profil kiberbiztonsági vonatkozású összetevői, komponensei. Forrás: NIST, Baldrige Cybersecurity Excellence Builder, DRAFT.

(Framework for Improving Critical Infrastructure Cybersecurity, by NIST) – Keretrendszer szempontjai alapján és elemeinek figyelembe vételével került kidolgozásra a NIST által.

7.2 Kik a potenciális felhasználói az eszköznek?

- Az Igazgatótanács és az igazgatók, végrehajtó menedzserek, vezetők
- Az Informatikai igazgató (CIO)
- Az információbiztonsági vezető (CISO)
- Az IT folyamatgazdák és folyamat menedzserek
- KOCKÁZATKEZELÉSI SZERVEZETÍEK ÉS –SZAKEMBEREK, AUDITOROK

- Jogi megfelelőségi (Compliance) szervezetek és menedzserek
- Alkalmazottak, munkatársak

7.3 Hogyan használhatják a szervek, szervezetek az eszköz t a kiberbiztonsági kockázatok menedzselésének felmérésének és fejlesztésének érdekében?

Alapvetően 17 tétel (plusz 2 a „Szervezeti környezet"-témakörben), mindegyik elem területi fókusszal. Ezek az elemek három csoportra oszthatók az információk típusától függően, amelyekre vonatkozóan kérdéseket fogalmaznak meg:

7.3.1 Szervezeti környezet (C) amely a kiberbiztonsági kockázatkezeléssel kapcsolatos szervezeti információk és annak környezete.

7.3.2 Folyamat elemek (1-6 kategória), a kérdések a szervezet kiberbiztonsági folyamatokra irányulnak.

1. Vezetés, Leadership
2. Stratégia, Strategy
3. Ügyfelek, Customers
4. Mérés, Elemzés és Tudásmenedzsment
5. Munkaerő
6. Működés, Operations

7.3.3 Eredmény elemek (7. kategória) kérdései a szervezet kiberbiztonsági folyamataival kapcsolatos eredmények jelentéseire irányulnak.

7.3.4 Az Értékelő fejezet (az eredeti dokumentum 25. oldalán található) segít értékelni a kiberbiztonsági folyamatok hatékonyságát és eredményességét – csakúgy, mint a Kiberbiztonsággal kapcsolatos elért eredmények minőségét és ezek összességét – azaz hogyan működnek ezek rendszerként.

7.4 Az eszköz „Használati Utasítása” – Hogyan használhatjuk, melyek a lépései a kiberbiztonsággal kapcsolatos erőfeszítések értékelési folyamatának?

7.4.1 A felmérés hatókörének megállapítása: mi képezi a vizsgálat tárgyát?

A *Baldrige Cybersecurity Excellence Builder – a legértékesebb önértékelési eszköz egy teljes szervezet kiberbiztonsági kockázat menedzsment programjának értékelésére, de alkalmas* és hasznos lehet egy szervezeti egység, vagy több szervezeti egységből álló csoport, szervezeti részek felmérésére is.

7.4.2 A szervezeti környezet meghatározása, a kérdések megválaszolása

A szervezeti környezet c. fejezet kritikus fontosságú az alábbi okokból:

- Segít azonosítani az esetleges eltéréseket a kulcs információk és a kulcs kiberbiztonsági teljesítőképességi követelmények és eredmények között.
- ***Használhatjuk kezdeti/első felmérés eszközekénz is (baseline – alapvonal). A kérdések megválaszolása során felmerülő esetleges ellentmondásos területek, vagy kiderülő hibák, illetve hiányosságok (információk vagy megoldások hiánya) azonosítása segítségével akcióterv alkotható ezek megszüntetésére, fejlesztésre, előre lépésre.***
- Meghatározza a kontextust és lehetővé teszi, hogy feltárjuk az adott szervezet speciális, egyedi vonásait, kiberbiztonsággal kapcsolatos igényeit, a többi Baldrige Cybersecurity Excellence Builder kérdésre adott válasz segítségével.

7.4.3 - A 7.3.2 pont Az 1-6. kategória kérdéseinek megválaszolása

Sok kérdés „Hogyan”-nal kezdődik. Ezeknek a hogyanoknak a megválaszolása során fontos információkat adunk az adott szervezet kiberbiztonsággal kapcsolatos *kulcs folyamatairól:* ***(M-H-TK-I)***

- ***Megközelítés*** *(Approach): Hogyan történik a szervezet kiberbiztonsággal kapcsolatos feladatainak végrehajtása? Mennyire szisztematikusak (rendszeresek, módszeresek) a meglévő kulcsfolyamatok?*
- ***Használat, elterjesztés*** *(Deployment): Mennyire következetesen használják a kiberbiztonsággal kapcsolatos kulcsfolyamatokat a szervezet releváns szervezeti egységei?*

- ***Tanulás és kommunikáció*** *(Learning): Értékelték és továbbfejlesztették az adott szervezet* kiberbiztonsággal kapcsolatos *kulcsfolyamatait?* Az eredményeket megosztották a szervezeten belül?
- ***Integráció*** *(Integration): Mennyire fedi le a kiberbiztonsággal kapcsolatos folyamatok kezelése a jelenlegi és jövőbeli szervezeti igényeket, követelményeket?*

A 7.4.4 – A 7.3.3 pont – a 7. kategória kérdéseinek megválaszolása

Ezekben az elemekben információt adunk a kérdések megválaszolásával azokról a Kiberbiztonsággal kapcsolatos eredményekről, amelyek a legfontosabbak szervezet sikeressége szempontjából: **(SZTÖI)**

- ***SZINTEK****/(Levels): Melyek a kulcs mutatói, mérőszámai a kiberbiztonsággal kapcsolatos folyamatok hatékonyságnak és eredményességének, mi a kiberbiztonsági teljesítmény, teljesítőképesség aktuális szintje?*
- ***TRENDEK****/(Trends): Az eredmények fejlődő, stagnáló vagy hanyatló, visszaeső tendenciát mutatnak?*
- ***ÖSSZEHASONLÍTÁSOK****/(Comparisons): Milyen a szervezet helyzete, eredményei kiberbiztonság tekintetében más szervezetekhez, versenytársakhoz képest, vagy Összemérés (Banchmarking) tekintetében?*
- ***INTERGRÁCIÓ****/(Integration): A kiberbiztonsággal kapcsolatos - a szervezet szempontjából fontos eredményeket monitorozzák és rögzítik? Figyelembe veszik a tulajdonosok és a kulcs személyes igényeit, elvárásait? Figyelembe veszik aza eredményeket a döntéshozatali folyamatokban?*

7.4.5 Alkalmazzunk egy LEÍRÓT minden egyes kérdés elemre adott válasz során

Az eredeti dokumentumban a 25. 26. oldalon lévő folyamat és az eredmények fejezetek használatával rendeljünk hozzá egy leírót, amely lehet: - **Reaktív, Korai, Fejlett vagy Szerep modell** - leíró társítása minden válaszhoz.

7.4.6 Priorizáljunk, rangsoroljunk minden tevékenységet

Jelezzük a fontosságot is (Magas, Közepes, Alacsony) minden egyes elemre, kérdésre adott válasz során a sikeres kiberbiztonsági menedzsment érdekében.

A kiberbiztonsági kockázatkezelési program erősségeire alapozva, fejlesszük tovább az elért eredményeket. Ezeknek az erősségeknek és eredményeknek a többi szervezeti egységgel való megosztása révén felgyorsíthatjuk a fejlesztés folyamatát.
Állítsuk rangsorba a lehetőségeket, a kiberbiztonsági folyamatok és eredmények fejlesztendő területeit is: mivel lépésenként haladhatunk csak, nem tudunk mindent egyszerre végrehajtani. Gondoljuk meg melyek a szervezet szempontjából legfontosabbak jelenleg. Teremtsünk egyensúly a tulajdonosi, vezetői igények és elvárások és a lehetséges erőforrásokkal elérhető elvárható eredmények között és döntsük el a végrehajtási sorrendet, mit hajtsunk végre először.

8. Dolgozzunk ki akciótervet, valósítsuk meg, mérjük és értékeljük az előrehaladást

Ahogy reagálunk a kérdésekre és felmérjük a válaszokat az adott fejezetben, akkor kezdjük beazonosítani az erősségeket és gyenge pontokat, először a kategóriákon belül, majd azok között is. Hangoljuk össze, koordináljuk a legfontosabb folyamatok közötti kapcsolatokat, továbbá a folyamatok és az eredmények közötti összefüggéseket, ezek vezethetnek el javítási ciklusokhoz.
Az eszköz további folyamatos használata során egyre többet és többet tudhatunk meg szervezetünkről és meghatározhatjuk az erősségekre építés, az eltérések megszüntetésének és az innováció legjobb módját.
Ennek az önértékelésnek a teljesítésével megtehetjük az első lépést, megfelelve és eleget téve a *Cybersecurity Framework,* section 3.0 pontjában javasoltaknak: (“How to Use the Framework” – Hogyan használjuk a keretrendszert):

8.2 A kiberbiztonsági folyamatok alapvető felmérése, áttekintése

Az önértékelési eszköz kérdéseire adott válaszok során szerzett információkat hasonlítsuk össze az aktuális tevékenységeinket azokkal a kiberbiztonsági tevékenységekkel, amelyek a „*Cybersecurity Framework* Core” dokumentumban szerepelnek.

8.3 Kiberbiztonsági program létrehozása vagy továbbfejlesztése

Használjuk a válaszokat, amelyeket az önértékelési kérdésekre adtunk, hogy tájékoztassuk a hét lépés létrehozásában vagy bővítésében a kiberbiztonság program tekintetében. (lásd a mellékletet).

8.4 A kiberbiztonsági követelmények kommunikációja a tulajdonosokkal, vezetőkkel

A kérdésekre adott válaszok segítségünkre lehetnek egy „Célprofil" létrehozásában és az egyeztetésben a menedzserekkel, vezetőkkel, tulajdonosokkal, döntéshozókkal a kiberbiztonsági kockázatkezelési követelményrendszer tekintetében.

9. SZK – Szervezeti környezet („C" – as Context in original document)

SZK.1 A szervezet leírása: Melyek a szervezet kulcs karakterisztikái?

a. Szervezeti környezet

(1) TERMÉKEK ÉS SZOLGÁLTATÁSOK

(2) KÜLDETÉS, JÖVŐKÉP ÉS ÉRTÉKEK

(3) MUNKAERŐ PROFIL

(4) VAGYONTÁRGYAK, ESZKÖZÖK

(5) JOGI ÉS SZABÁLYZATI KÖVETELMÉNYEK

b. Szervezeti kapcsolatok

(1) Szervezeti Struktúra

(2) Ügyfelek és érdekeltek

(3) Szállítók és Partnerek

TÁBLÁZATOK ÉS MUNKALAPOK [16]

Értékelési kategóriák (1-6.) Folyamatok [16]

Process (Categories 1–6)

Maturity Level	Evaluation Factor			
	Approach	Deployment	Learning	Integration
Reactive	CYBERSECURITY-related policies/operations are characterized by activities rather than by PROCESSES.	DEPLOYMENT of CYBERSECURITY-related APPROACHES to appropriate organizational units, and to CUSTOMERS, PARTNERS, and suppliers, as appropriate, is lacking.	Improvement in CYBERSECURITY-related policies/operations is achieved mainly in reaction to immediate needs or problems.	CYBERSECURITY-related goals are poorly defined; individual units within the CYBERSECURITY operations function independently of each other. There is no coordination between CYBERSECURITY-related policies/operations and those of the rest of the organization.
Early	CYBERSECURITY-related policies/operations are beginning to be carried out with SYSTEMATIC APPROACHES.	KEY CYBERSECURITY-related APPROACHES are beginning to be DEPLOYED to appropriate organizational units and to CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are beginning to be SYSTEMATICALLY evaluated and improved.	CYBERSECURITY-related strategy and quantitative GOALS are being defined. There is some early alignment among CYBERSECURITY operational units and, as appropriate, between CYBERSECURITY policies/operations and the rest of the organization.
Mature	Most elements of CYBERSECURITY-related policies/operations are characterized by SYSTEMATIC APPROACHES.	KEY CYBERSECURITY-related APPROACHES are well DEPLOYED to appropriate organizational units and to CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are SYSTEMATICALLY evaluated for improvement, and learnings are shared, with some INNOVATION evident.	CYBERSECURITY-related APPROACHES address KEY strategies and GOALS. There is alignment among CYBERSECURITY operational units and, as appropriate, between CYBERSECURITY policies/operations and the rest of the organization.
Role Model	Many to all elements of CYBERSECURITY-related policies/operations are characterized by SYSTEMATIC APPROACHES.	KEY CYBERSECURITY-related APPROACHES are fully DEPLOYED to appropriate organizational units and to CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations seek and achieve efficiencies through ANALYSIS, INNOVATION, and the sharing of CYBERSECURITY information and knowledge, including with the rest of the organization.	CYBERSECURITY-related policies/operations are INTEGRATED with current and future organizational needs defined by the organization; these policies/operations are well INTEGRATED with those of the rest of the organization.

Értékelési kategória (7. Eredmények) [16]

Results (Category 7)

Maturity Level	Evaluation Factor			
	Levels	Trends	Comparisons	Integration
Reactive	CYBERSECURITY-related RESULTS are missing, not used, or randomly reported.	TREND data are not reported or show mainly adverse TRENDS.	Available comparative information is not tracked.	CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are not tracked.
Early	The organization tracks some CYBERSECURITY-related RESULTS, and they show early good performance LEVELS.	Some TREND data are tracked, and some show improvement over time.	Some available, mainly internal, comparative information is tracked.	Some CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are tracked.
Mature	The organization tracks many CYBERSECURITY-related RESULTS, and they show good-to-excellent performance LEVELS.	Many CYBERSECURITY-related RESULTS show improvement or sustained high PERFORMANCE over time.	Results show good CYBERSECURITY-related PERFORMANCE relative to available information on competitors, other relevant organizations, or BENCHMARKS.	Many CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are tracked. RESULTS are beginning to be used in decision making.
Role Model	The full array of CYBERSECURITY-related RESULTS is tracked, indicating top performance.	The full array of CYBERSECURITY-related RESULTS is TRENDED over time, indicating improvement or sustained high PERFORMANCE.	Results indicate top CYBERSECURITY-related PERFORMANCE relative to available information on other organizations or BENCHMARKS.	All CYBERSECURITY-related RESULTS that are important to the organization's ongoing success are tracked. The RESULTS are used in decision making.

Az önértékelési táblázatok [16]

Self-Analysis Worksheet

[Note: In its final form, this worksheet may be an Excel file with drop-down boxes and/or another type of non-paper-based tool.]

Process (Categories 1–6)	Reactive, Early, Mature, or Role Model?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
1 Leadership					
1.1 Senior and Cybersecurity Leadership: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?					
1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and fulfill your organization's societal responsibilities?					
2 Strategy					
2.1 Strategy Development: How do you develop your cybersecurity strategy?					
2.2 Strategy Implementation: How do you implement your cybersecurity strategy?					
3 Customers					
3.1 Voice of the Customer: How do you obtain information from your customers?					
3.2 Customer Engagement: How do you engage customers by serving their needs and building relationships?					
4 Measurement, Analysis, and Knowledge Management					
4.1 Measurement, Analysis, and Improvement of Performance: How do you measure, analyze, and then improve cybersecurity-related performance?					
4.2 Knowledge Management: How do you manage your organization's cybersecurity-related knowledge assets?					
5 Workforce					
5.1 Workforce Environment: How do you build an effective and supportive workforce environment to achieve your cybersecurity goals?					
5.2 Workforce Engagement: How do you engage your workforce to achieve a high-performance work environment in support of cybersecurity policies and operations?					
6 Operations					
6.1 Work Processes: How do you design, manage, and improve your key cybersecurity work processes?					
6.2 Operational Effectiveness: How do you ensure effective management of your cybersecurity operations?					

Results (Category 7)	Reactive, Early, Mature, or Role Model?				High, Medium, or Low?
	Levels	Trends	Comparisons	Integration	Importance
7 Results					
7.1 Cybersecurity Process Results: What are your cybersecurity performance and process effectiveness results?					
7.2 Customer Results: What are your customer-focused cybersecurity performance results?					
7.3 Workforce Results: What are your workforce-focused cybersecurity performance results?					
7.4 Leadership and Governance Results: What are your cybersecurity leadership and governance results?					
7.5 Financial Results: What are your financial performance results for your cybersecurity operations?					

Evaluating Your Responses

1. **For each item (e.g., 1.1, 1.2) in categories 1–7 of the *Baldrige Cybersecurity Excellence Builder*, use the process and results rubrics on pages 24–25 to assign a descriptor (Reactive, Early, Mature, or Role Model) for each evaluation factor.**

For processes (categories 1–6), the evaluation factors are approach, deployment, learning, and integration (ADLI):

- *Approach* consists of the methods used to carry out a process, the degree to which your approach is systematic (i.e., repeatable and based on reliable data and information), the appropriateness of these methods to the item questions and your operating environment, and the effectiveness of your use of the methods.
- *Deployment* is the extent to which your approach is applied consistently and the extent to which it is used by all appropriate work units.
- *Learning* is the refinement of your approach through cycles of evaluation and improvement, the encouragement of breakthrough change to your approach through innovation, and the sharing of refinements and innovations with other relevant work units and processes in your organization.
- *Integration* is the extent to which your approach is aligned with the organizational needs identified in the Organizational Context section and in other process items. Integration also includes the extent to which your measures, information, and improvement systems are complementary across processes and work units; and the extent to which your plans, processes, results, analyses, learning, and actions are harmonized across processes and work units to support organization-wide goals.

For results (category 7), the evaluation factors are levels, trends, comparisons, and integration (LeTCI; "let's see").

- *Levels* are your current performance on a meaningful measurement scale.
- *Trends* are your rate of performance improvement or continuation of good performance in areas of importance (i.e., the slope of data points over time).
- *Comparisons* are your performance relative to that of other, appropriate organizations, such as competitors or organizations similar to yours, and your performance relative to industry leaders or relevant benchmarks.
- *Integration* is the extent to which your results address important performance requirements relating to customers, products/services, markets, processes, and action plans identified in the Organizational Context section and in the process items (categories 1–6). It also includes the extent to which your results reflect harmonization across your processes and work units to support organization-wide goals.

2. **Indicate the importance (high, medium, or low) of each item to the successful management of cybersecurity within your organization.**
3. **Prioritize your actions.**

Celebrate your strengths of your cybersecurity risk management program, and build on them to improve what you do well. Sharing the things you do well with the rest of your organization can speed improvement.

Prioritize your opportunities for improvement; you cannot do everything at once. Think about what is most important for your organization as a whole at this time, balancing the differing needs and expectations of your stakeholders, and decide what to work on first. Look at the next level in the rubric for how you might improve. Develop an action plan, implement it, and measure your progress.

Függelék a Baldrige Cybersecurity Excellence Builderhez [16]

Táblázat: Az eszköz és a Cybersecurity Framework kapcsolata, összefüggései

Cybersecurity Excellence Builder Categories and Items	Related Sections in the *Cybersecurity Framework*		
	2.4, Figure 2: Notional Information and Decision Flows	3.2, Establishing or Improving a Cybersecurity Program	Appendix A: Framework Core Categories and Functions[1]
C Organizational Context			
C.1 Organizational Description	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-AM, ID-BE
C.2 Organizational Situation	Executive Level; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, ID-RM
1 Leadership			
1.1 Senior and Cybersecurity Leadership	Executive Level	Step 1: Prioritize and Scope; Step 2: Orient	ID-BE, RC-CO
1.2 Governance and Societal Responsibilities	Executive Level	Step 2: Orient	ID-GV, RS-CO
2 Strategy			
2.1 Strategy Development	Business/Process Level; Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient; Step 4: Conduct a Risk Assessment; Step 5: Create a Target Profile Step 6: Determine, Analyze, and Prioritize Gaps	ID-BE, ID-GV, ID-RA, ID-RM
2.2 Strategy Implementation	Business/Process Level; Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	Step 1: Prioritize and Scope; Step 2: Orient; Step 5, Create a Target Profile; Step 7: Implement Action Plan	ID-BE, ID-GV, ID-RA, ID-RM
3 Customers			
3.1 Voice of the Customer	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	ID-BE
3.2 Customer Engagement	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	ID-AM, PR-AT, RS-CO, RC-CO
4 Measurement, Analysis, and Knowledge Management			
4.1 Measurement, Analysis, and Improvement of Performance	Implementation Progress	Step 6: Determine, Analyze, and Prioritize Gaps	DE-AE, DE-DP, RS-IM, RC-IM
4.2 Knowledge Management	Business/Process Management; Implementation/Operations Level	Step 6: Determine, Analyze, and Prioritize Gaps	ID-RA, DE-AE, RS-CO
5 Workforce			
5.1 Workforce Environment	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	ID-AM, ID-GV, PR-IP, DE-DP, RS-CO
5.2 Workforce Engagement	Business/Process Management; Implementation/Operations Level	Step 3: Create a Current Profile; Step 5: Create a Target Profile	PR-AT, PR-IP, RS-CO

6	**Operations**			
	6.1 Work Processes	Implementation/Operations Level	Step 2: Orient; Step 3: Create a Current Profile; Step 4, Conduct a Risk Assessment; Step 5, Create a Target Profile	PR-AC, PR-DS, PR-IP, PR-MA, DE-AE, DE-CM, DE-DP, RS-RP, RS-AN, RS-IM, RS-MI, RC-RP, RC-IM
	6.2 Operational Effectiveness	Implementation/Operations Level	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-AM, ID-BE, PR-AT, PR-IP
7	**Results**			
	7.1 Process Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	PR-AC, PR-DS, PR-IP, PR-MA, DE-AE, DE-CM, DE-DP, RS-RP, RS-AN, RS-IM, RS-MI, RC-RP, RC-IM
	7.2 Customer Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-BE, ID-AM, PR-AT, RS-CO, RC-CO
	7.3 Workforce Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-AM, ID-GV, PR-IP, DE-DP, RS-CO, PR-AT, PR-IP, RS-CO
	7.4 Leadership and Governance Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-BE, ID-GV, ID-RA, ID-RM, RC-CO
	7.5 Financial Results	Implementation Progress	Step 3: Create a Current Profile; Step 5, Create a Target Profile	ID-BE

[1]The *Cybersecurity Framework* functions are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). For an explanation of the categories within these functions, see the *Cybersecurity Framework*.

10. Forrásmunkák, linkek, referenciák:

Internetes források:

1. NIST Cybersecurity Excellence builder tool:
https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf

2. NIST Cybersecurity Framework
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

3. NIST Cybersecurity Framework (CSF) **CORE** Reference Tool

- NIST Cybersecurity Framework (CSF) Reference Tool
nist.gov/cyberframework/csf_reference_tool.cfm

The NIST CSF reference tool is a FileMaker runtime database solution. It represents the FrameworkCore which is a set of cybersecurity activities etc.

4. Published more than 40 different standards and guidelines to help protect non-national security IT systems from cyber threats.

A kiberfenyegetések elleni védelem NIST által kiadott több mint 40 szabványa és irányelve:
https://www.nist.gov/cybersecurity-1

5. NIST Special Publication (Second draft) 800-150 34 35 36 Guide to Cyber Threat Information Sharing. A kiberfenyegetésekkel kapcsolatos információk megosztása:
http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf

6. NIST - Computer Security Resource Center – Az USA Nemzeti Szabványügyi Hivatalának linkje:

http://csrc.nist.gov/

7. CYBEREYE Blog archive link:
https://gcn.com/blogs/cybereye/2016/09/nist-cyber-self-assessment.aspx?s=gcntech_300916&mkt_tok=eyJpIjoiTWpVNU9EbGpNV1ZoWTJRdyIsInQiOiJ1YnNWZVFBclg5ZXZ2NHRHYWErQjVwN1ZBYitEUzUrWmZoMUJSaGtTTWk3emZuNzlFUUlTTlIxVUhEMXRGMjJFK3lOSnJmYVhmY0pRTFNVYlZOOUNDRlpzT3ZPMFFoemZrRVI2aVM1TzdXbz0ifQ%3D%3D

8. Index.hu cikk: Az Európai Unió Hálózatbiztonsági irányelve (NIS):
http://index.hu/tech/2016/08/08/europa_kiberbiztonsag_halozatvedelem_nis_iranyelv/

9. NATO Tanulmány a magyar kiberbiztonsági helyzetről
https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf

10. Index.hu cikk: Egy kézben a magyar kibervédelem
http://index.hu/tech/2015/11/03/egy_kezben_a_magyar_kibervedelem/

11. Magyarország kibervédelmi stratégiája:
http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845

12. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323157

13. 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
http://njt.hu/cgi_bin/njt_doc.cgi?docid=165583.269327

14. Index.hu cikk: Munkacsoportok? Megvannak. Biztonság? Dolgozunk rajta
http://index.hu/tech/2016/09/29/munkacsoportok_megvannak_biztonsag_dolgozunk_rajta/

A magyarországi kormányzati kiberkoordináció helyzete, az állami és piaci szereplők együttműködésének formái.

15. Index.hu cikk: Európa felkészül a kiberháborúra;
http://index.hu/tech/2016/08/08/europa_kiberbiztonsag_halozatvedelem_nis_iranyelv/

16. A Baldridge Excellence Framework – A Baldrige Kiválósági Keretrendszer
https://www.nist.gov/baldrige/publications/baldrige-excellence-framework

17. A Baldridge Excellence Builder Tool
https://www.nist.gov/sites/default/files/documents/baldrige/publications/Baldrige_Excellence_Builder.pdf

MELLÉKLET:

Minősített adatokat (is) kezelő szervezetek és rendszerek kiberbiztonsági szempontú kockázatelemzését, fejlettségi szintjének felmérését támogató modell és módszertani segédeszköz.

Egy Excel alapú táblázatos pontozásos vegyes (kvalitatív-kvantitatív) kockázatelemzési módszertanon alapuló megoldás. A „CD RISKMAN" – CYBER DEFENCE RIKS ASSESSMENT AND MANAGEMENT TOOLSET. Egy elsősorban de nem kizárólag - minősített adatokat kezelő szervezetek és rendszerek kiberbiztonsági szempontú kockázatelemzését, fejlettségi szintjének felmérését támogató modell és módszertani segédeszköz.

1. A SZERVEZETI KIBERKOCKÁZATI PROFIL – A KOCKÁZATI KITETTSÉG MÉRTÉKE ÉS MÉRÉSE

Egy szervezetet és annak komplex kiberbiztonsági és (minősített) adatkezelési szempontú kockázati kitettségét ezzel a jellemzővel határozhatjuk meg. Ezt KIBERBIZTONSÁGI KOCKÁZATI PROFILNAK (KP), vagy röviden kiberkockázati profilnak nevezzük. Ez a kiberkockázati profil jellemző az adott szervre, szervezetre, telephelyre, adatkezelő környezetre, rendszerre, annak komplex kiberkockázati szintjére.

A modell jelenleg és jellemzően 5 kategóriából, és ezeken belül a kockázatot befolyásoló tényezőkből áll össze, melyek bármelyikének megváltozása befolyásolja (módosítja!) az adott szervezet kiberbiztonsági kockázati profilját. A szervezeti kiberkockázati kitettség mértéke egy számszerűsített jellemző, amely jellemző az adott szervezet és rendszer minősített adatkezelési szempontú kiberbiztonsági kockázat nagyságára a fenyegetettségekkel és a sebezhetőségekkel arányosan. **Ez lehet Minimális, Alacsony, Közepes, vagy Magas, illetve MAXIMÁLIS/IGEN MAGAS.**

2. KIBERBIZTONSÁGI SZEMPONTÚ SZERVEZETI-RENDSZER KOCKÁZATI SZINTEK MEGHATÁROZÁSA

2.1 Az összesített kiberbiztonsági kockázati profil szintjei

2.1.1 Minimális szintű kiberbiztonsági kockázati profil

Egy szervezet esetén ez a szint nagyon korlátozott IT/technológiahasználatot jelent. Alacsony komplexitású és igen kisszámú informatikai (IT) rendszerrel, berendezéssel rendelkeznek (1-2). Minimális a számítógépek, az alkalmazások és az eszközök száma. A kezelt minősített adatok érzékenységi szintje igen alacsony (Korlátozott Terjesztésű vagy alacsonyabb). Kevés alkalmazott (max. 1-2 fő) fér hozzá minősített adatokhoz és a kezelt minősített dokumentumok száma is minimális (<5 dokumentum/hónap) . A szervezet geográfiai „lábnyoma" és digitális lenyomata is elenyésző.

2.1.2 Alacsony szintű kiberbiztonsági kockázati profil

Ezen a szinten lévő szervezetek korlátozott komplexitású és viszonylag kisszámú IT rendszerrel, berendezéssel, minősített adatot kezelő berendezéssel, eszközzel rendelkeznek (n>2). A kezelt minősített adatok érzékenységi szintje és kritikussága viszonylag alacsony (Bizalmas vagy alacsonyabb). A kezelt minősített dokumentumok száma <15/hónap. Viszonylag kevesen férnek hozzá minősített adatokhoz (2-5 fő). A szervezet geográfiai és digitális lábnyoma alacsony mértékű.

2.1.3 Közepes szintű kiberbiztonsági kockázati profil

Ezen a szinten lévő szervezetek közepes komplexitású és közepes számú IT rendszerrel, berendezéssel, minősített adatot kezelő berendezéssel, eszközzel rendelkeznek (2>n>5). A kezelt minősített adatok érzékenységi szintje és kritikussága közepes (TITKOS vagy alacsonyabb). A kezelt minősített dokumentumok száma <25/hó. Viszonylag kevesen férnek hozzá minősített adatokhoz (5-8 fő). A szervezet geográfiai és digitális lábnyoma közepes mértékű.

2.1.4 MAGAS kiberbiztonsági kockázati profil

Ezen a szinten lévő szervezetek jelentős komplexitású és számú rendszerrel, berendezéssel, minősített adatot kezelő eszközzel/rendszerrel rendelkeznek (5>n<10 az eszközök száma). A kezelt minősített adatok érzékenységi szintje és kritikussága közepes (TITKOS vagy magasabb). A kezelt

minősített dokumentumok száma: n<50/hó. Viszonylag kevesen férnek hozzá minősített adatokhoz (n<10 fő). A szervezet geográfiai és digitális lábnyoma jelentős mértékű.

2.1.5 Maximális, IGEN MAGAS szintű kiberbiztonsági kockázati profil

Ezen a szinten lévő (nagy és/vagy kiemelt fontosságú, kritikus, létfontosságú) szervezetek nagy komplexitású és számú rendszerrel, berendezéssel, minősített adatot kezelő rendszerrel és eszközzel rendelkeznek (n>10). A kezelt minősített adatok érzékenységi szintje és kritikussága igen magas (SZIGORÚAN TITKOS). A kezelt minősített dokumentumok száma >50/hó. Viszonylag sokan férnek hozzá minősített adatokhoz (n>10 fő). A szervezet geográfiai és digitális lábnyoma nagymértékű.

3. A MÓDSZERTAN ÉS AZ ESZKÖZ – „CD-RISKMAN" átfogó ismertetése

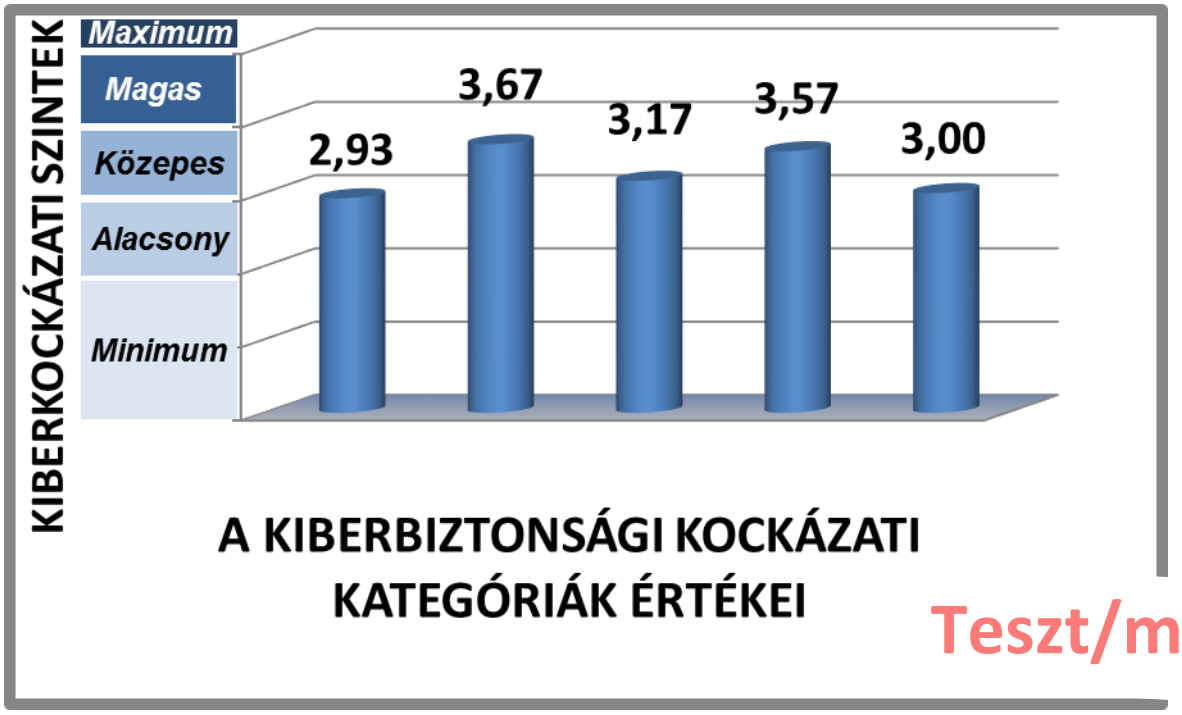
Minősített adatkezelő rendszerek és szervezetek kiberbiztonsági szempontú kockázatelemzése és fejlettségének értékelése.

3.1 A kockázati szintek és kategóriák összefoglaló ábrázolás

RENDSZERKOCKÁZAT Profil (Kategória szerint)	RENDSZER-KOCKÁZATI SZINT	Normalizált Kockázat Pontszám	Kockázat Pontszám	A tényezők száma #
1. LÉTESÍTMÉNY-, KÖRNYEZETI- ÉS RENDSZERJELLEMZŐK	*Közepes*	2,93	*41*	14
2. (MINŐSÍTETT) ADATOK ÉS ADATHORDOZÓK	*Magas*	3,67	11	3
3. (MINŐSÍTETT) ADATFELDOLGOZÓ RENDSZEREK KÖVETELMÉNYEK ÉS ELEMEK	*Közepes*	3,17	38	12
4. SZERVEZET, EMBEREK ÉS KAPCSOLATOK	*Magas*	3,57	25	9
5. FENYEGETETTSÉGEK, SEBEZHETŐSÉGEK	*MAXIMUM*	4,50	6	3
KIBERBIZTONSÁGI ÖSSZKOCKÁZATI SZINT	*KÖZEPES*	*3*	121	41

KIBERBIZTONSÁGI FEJLETTSÉGI SZINTEK		KÍVÁNT SZINTEK		
Fejlődő	MINIMUM SZINT			
Közepes	OPTIMUM SZINT			
Magas	MAXIMUM SZINT			

3.2 A kiberbiztonsági kockázati szintek és értékeik



3.3 A kiberbiztonsági kockázati kategóriák

1.LÉTESÍTMÉNY, KÖRNYEZETI ÉS RENDSZERJELLEMZŐK
2. (MINŐSÍTETT) ADATOK ÉS ADATHORDOZÓK
3. (MINŐSÍTETT) ADATFELDOLGOZÓ RENDSZEREK, KÖVETELMÉNYEK ÉS ELEMEK
4. SZERVEZET, EMBEREK ÉS KAPCSOLATOK
5. FENYEGETETTSÉGEK, SEBEZHETŐSÉGEK

4. FEJLETTSÉGI MODELL SZINTEK

A fejlettségi modell szintek az alábbiak

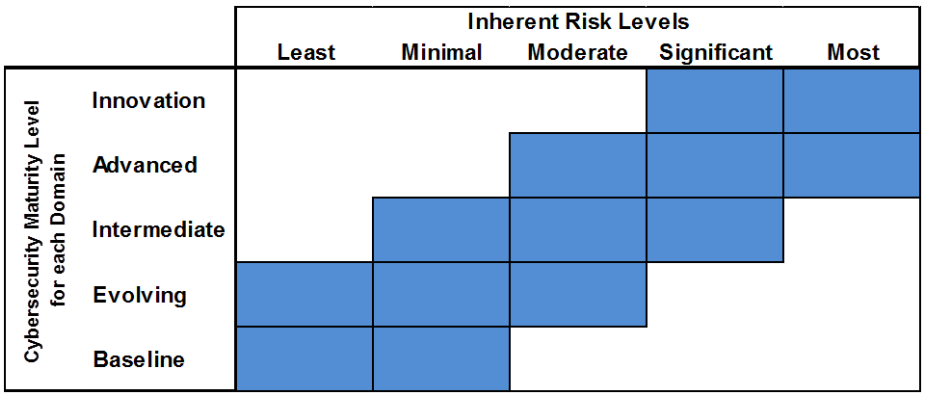
Baseline - ALAPVONAL

Evolving - Fejlődő

Intermediate - Közepes

Advanced – Magas

Innovation – Innovatív



Az ábra az FFIEC Cyberrisk Management Maturity Modellje alapján került másolásra és alkalmazásra

SAJÁT Táblázat:

4.1 A fejlettségi kategóriák és értékelési faktoraik

FEJLETTSÉGI KATEGÓRIA	Értékelési Faktorok	Kívánt Érettségi szint Kategóriánként
K1: KOCKÁZAT KEZELÉS & IRÁNYÍTÁS	1: VEZETŐI IRÁNYÍTÁS	**Evolving - Fejlődő**
	2: KOCKÁZATKEZELÉS	
	3: ERŐFORRÁSOK	
	4: Képzés & Kultúra	
K2: Fenyegetettség-Veszélyelemzés	1: Fenyegetettségelemzés	**Advanced - Magas**
	2: Veszélyelemzés	
	3: Információ szerzés és megosztás	
K3: Biztonsági kontrollok	1: Preventiv Kontrollok	**Intermediate - Közepes**
	2: Detectív Kontrollok	
	3: Korrectív Kontrollok	
K4: Külső függőség Menedzsment	1: KAPCSOLATOK	**Evolving - Fejlődő**
	2: Ralációmenedzsment	
K5: Incidens Menedzsment	1: Incidenskezelés Tervezés és Stratégia	**Evolving - Fejlődő**
	2: Detektálás, Válaszadás és Hatáscsökkentés	
	3: Eszkalálás és Jelentés	

SAJÁT TÁBLÁZAT:

4.2 A FEJLETTSÉGI KATEGÓRIÁK ELEMEI

K1: KOCKÁZATKEZELÉS & IRÁNYÍTÁS
1: VEZETŐI IRÁNYÍTÁS
2: KOCKÁZATKEZELÉS
3: ERŐFORRÁSOK
4: Képzés & Kultúra
K2: Fenyegetettség- Sebezhetőségelemzés
1: Fenyegetettségelemzés, veszélyelemzés és veszélykezelés
2: Sebezhetőségelemzés és kezelés
3: Információszerzés és megosztás
K3: Biztonsági kontrollok – kockázatkezelő intézkedések
1: Preventiv Kontrollok
2: Detectív Kontrollok
3: Korrectív Kontrollok
K4: Külső függőség menedzsment
1: KAPCSOLATOK
2: Ralációmenedzsment
K5: Incidens Menedzsment
1: Incidenskezelés Tervezés és Stratégia
2: Detektálás, Válaszadás és Hatáscsökkentés
3: Eszkalálás és Jelentés

5. A KOCKÁZATI KITETTSÉG SZINTJEI

A FENTI KATEGÓRIÁK SZERINTI JELLEMZŐKET AZ ALÁBBI 5 SZINTNEK MEGFELELŐEN KELL PONTOZNI A MEGHATÁROZOTT KRITÉRIUMOK ALAPJÁN.
A MÓDSZERTAN jelenlegi verziója 5 kockázati szintet különböztet meg, a finom felbontás érdekében ezeket pontszámokkal jellemezzük, súlyozzuk és pontozzuk.
A komplex kiberkockázati kitettséget - azaz a Szervezet és rendszereinek Kiberbiztonsági szempontú kockázati Profilját - ezek összegzésével és normalizált, súlyozott értékeinek számításával és kategorizálásával képezhetjük és jellemezzük.
A SZERVEZETRE JELLEMZŐ TELJES KIBERKOCKÁZATI PROFIL IS BESOROLHATÓ 5 KATEGÓRIÁBA AZ ÖSSZETEVŐK, A SÚLYTÉNYEZŐK (RELATÍV PREFERENCIA, FONTOSSÁGI SORREND) ÉS A HATÁRÉRTÉKEK ISMERETÉBEN, AZOK FÜGGVÉNYÉBEN.

A SZINTEK A KÖVETKEZŐK:

0 – Nem létező (Nem kitöltött az érték)
1 – Minimális kockázat (1 pont)
2 – Alacsony kockázat (2 pont)
3 – Közepes kockázat (3 pont)
4 – Magas, jelentős kockázat (4 pont)
5 – Maximális, igen magas kockázat (5 pont)

Az értékhatárok, a Kiberkockázati küszöbértékek az alábbiak.
Ezek a pontozásos értékelést követő számítás alapján a besorolás határértékei.

5.1 AZ ÉRTÉKHATÁROK

1.) **Minimális n < 1.5**
2.) **Alacsony: 1.5 < n <2.5**
3.) **Közepes: 2.5 < n < 3.5**
4.) **Szignifikáns: 3.5 ≤ n < 4.5**
5.) **Maximális n ≥ 4.5**

Ahol „n” a normalizált számított kiberkockázati érték.

6. KIBERBIZTONSÁGI KOCKÁZATKEZELÉS ÉS KOCKÁZAT-MENEDZSMENT

A vegyes kvantitatív-kvalitatív modell és módszertan alkalmazásával egy pontozásos és súlyozott normalizált kiberbiztonsági kockázati kitettség érték számításán alapuló megoldással pontos helyzetképet kaphatunk a kiberbiztonsági kockázatokról. Az Excel táblázatban kategóriánként strukturáltan szereplő és kitöltendő tényezők értékei az ún. Inherent Riskek, a technológia alkalmazásából adódó és a környezeti, szervezeti tényezők, valamint a(z) (minősített) adatok mennyisége és kezelésük módja, minősége által meghatározott és ezekből adódó komplex kiberbiztonsági kockázat meghatározásához szükséges kérdések és értékelésük, besorolásuk. (kockázati kritériumok).

A válaszok megadásával és ezek pontozásával, súlyozott értékük, valamint a küszöbértékek figyelembevételével – amelyeket statisztikai adatok és tapasztalati értékek, valamint a KIPA módszeren alapuló súlytényezők szakértői meghatározása alapján állítottunk össze – elvégezhető az EU-s és NATO-s és NEMZETI minősített adatok kezelése esetén kötelezően előírt – minősített adatok feldolgozásának kibervédelmi kockázatelemzése és értékelése. Ez lehet a kiberbiztonsági kockázatkezelés alapja.

A módszertan alkalmazásával automatizált módon – tehát a szubjektivitás és a hibalehetőségek, az emberi tényező kiküszöbölésével, illetve ezek minimálisra csökkentésével – szervezetenként összehasonlítható kiberkockázati kitettség értékek, ún „Kiberkockázati Profil”-ok (KP-k) határozhatók meg és az adott szervezet a jogszabály által meghatározott szintekbe sorolható. (3 szinten: Alacsony, Közepes vagy Magas, vagy a fenti 5 szintnek megfelelően: 1. Minimális, 2. Alacsony 3. Közepes. 4. Magas. 5. Maximális / IGEN MAGAS.

Az eszköz tartalmaz egy Fejlettségi szintet meghatározó lehetőséget is (Maturity Model) – amely az adott szervezet kibervédelmi fejlettségi szintjére jellemző. A kibervédelmi kockázati kitettség és a Fejlettségi szint között szoros összefüggés van, amely az eszköz alkalmazásával meghatározható, a kívánt mértékre beállítható – és az eredmények alapján Kiberbiztonsági kockázatkezelési akcióterv készíthető.

Ennek az eszköznek a segítségével eleget teszünk a nemzetközi követelményeknek és a kiberkockázati szempontú biztonsági szinteket átláthatóvá, kimutathatóvá, a kiberbiztonsági kockázatokat számszerűsíthetővé és összemérhetővé, kezelhetővé tesszük.

Nézetünk és törekvésünk szerint ez egy jelentős előrelépést jelenthet a hazai információ- és kiberbiztonsági szakmai színvonal emelése és a kockázati szempontú szemléletmód elterjesztése, fejlesztése terén is.