Az Európai Unió
Tanácsa

**Brüsszel, 2025. január 16.**
**(OR. en)**

**5426/25**

**CYBER 21**
**SAN 15**

**FEDŐLAP**

| | |
|---|---|
| Küldi: | az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató |
| Az átvétel dátuma: | 2025. január 15. |
| Címzett: | Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára |
| Biz. dok. sz.: | COM(2025) 10 final |
| Tárgy: | A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK<br>A kórházak és az egészségügyi szolgáltatók kiberbiztonságára vonatkozó európai cselekvési terv |

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: COM(2025) 10 final.

Melléklet: COM(2025) 10 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2025.1.15.
COM(2025) 10 final

# A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

## A kórházak és az egészségügyi szolgáltatók kiberbiztonságára vonatkozó európai cselekvési terv

## 1. Bevezetés

Az uniós biztonsági környezet gyors ütemben változik, és rohamosan elszaporodtak a hibrid és kibertámadások. Céljuk, hogy destabilizálják és megosszák társadalmunkat, és fennakadást idézzenek elő benne, de sokan a haszonszerzés céljával folytatnak kiberbűnözést. Európának ezért sürgősen fel kel készülnie ezen új valóságra, és reziliensebbé kell válnia vele szemben valamennyi ágazatban, összhangban a „társadalom egészére kiterjedő" és az „összkormányzati" megközelítéssel, aminek szükségére Sauli Niinistö, az Európai Bizottság elnökének különleges tanácsadója is felhívta a figyelmet.

A biztonságos és reziliens egészségügyi rendszerek az uniós társadalmi modell sarokköveit jelentik. A kórházak és az egészségügyi rendszerek ugyanakkor egyre több fenyegetéssel néznek szembe. Elsősorban zsarolóvírusossal dolgozó, pénzügyi haszonszerzés céljából működő bandák veszik őket célkeresztjükbe, mivel a betegadatok, többek között az elektronikus egészségügyi dokumentációk igen értékesek. Az elmúlt négy évben az egészségügyi ágazatot érte ténylegesen a legtöbb kibertámadás az Unióban, többek között a Covid19-világjárvány idején, amikor az egészségügyi infrastruktúra a szokásosnál többször vált kibertámadások célpontjává. A kórházak és az egészségügyi szolgáltatók elleni kibertámadások közvetlenül az embereknek ártanak, mivel hátráltatják az orvosi beavatkozásokat, akadályozzák a sürgősségi részlegek működését, sőt súlyos esetekben akár emberéletekbe is kerülhetnek.

A problémák pedig csak súlyosbodnak, mivel az ágazat elemi digitális átalakuláson megy keresztül. A digitális egészségügy, valamint az egészségügyi adatok felhasználása és továbbfelhasználása olyan ellátási modelleket tesz lehetővé, amelyek jobban igazodnak a betegek szükségleteihez és preferenciáihoz, mert segítik megelőzni a betegségek kialakulását és lehetővé teszik a kezelés korábbi megkezdését. A digitális eszközöknek és megoldásoknak a klinikai folyamatokba való integrálása, valamint az egészségügyi adatok felhasználása és továbbfelhasználása jobb klinikai döntésekhez vezethet, hozzájárulhat az egészségügy automatizálásához, valamint a betegek gyorsabb és jobb ellátásához. A digitális eszközök, az adatfelhasználás és a – gyakran internetkapcsolattal rendelkező és mesterséges intelligenciával (MI) működtetett – orvostechnikai eszközök kulcsfontosságúak az olyan kihívások kezelésében is, mint pl. a szakemberhiány az egészségügyben.

Ugyanakkor minden digitális eszköz újabb és újabb potenciális célpontot jelent a kiberbűnözők számára. Emellett egyes állami szereplők sem riadnak vissza attól, hogy egészségügyi létesítményeket vegyenek célba, amit Oroszország Ukrajna ellen folytatott agressziós háborúja is példáz. Így az ágazat egy kiterjedt hibrid hadviselés során kibertámadások lehetséges célpontjává válik. A kibertámadások nemcsak a betegbiztonságot veszélyeztetik, hanem aláássák a lakosság egészségügyi infrastruktúrába vetett bizalmát is, és jelentős helyreállítási költségekkel járnak. Az európai egészségügyi adattér[1] megvalósításának és teljes körű kiépítésének támogatásához a kibertámadások elhárításán felül elengedhetetlen, hogy reziliens és biztonságos digitális infrastruktúrával rendelkezzünk.

Ezért ideje, hogy fokozzuk és megerősítsük az európai kórházak és egészségügyi szolgáltatók kiberbiztonságát és rezilienciáját, amit Ursula von der Leyen elnök a 2024–2029-es Bizottság számára nyújtott politikai iránymutatásában[2] is hangsúlyozott. A helyzet sürgősségére és az ágazatot fenyegető

[1] https://www.consilium.europa.eu/hu/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.
[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_hu.

egyedi veszélyekre válaszul született meg ez a cselekvési terv. Az egészségügyi ellátási rendszer kiberbiztonsági kihívásainak megoldására nem létezik „csodafegyver”. Ehelyett a cselekvési terv arra szólít fel, hogy a megelőzésre, a felkészültségre és a szolidaritás összehangoltabb megközelítésére kell fókuszálni, az európai kiberbiztonsági ágazat szakértelmének kiaknázása mellett. A cselekvési terv a biztonsággal kapcsolatos uniós megközelítést követi, amelyet a kidolgozás alatt álló európai belső biztonsági stratégia még tovább fog fejleszteni és hivatalos formában is le fog fektetni. Ez utóbbi az összes belső biztonsági fenyegetésre kíván átfogó választ kidolgozni, középpontjában pedig azok a képességek fognak állni, melyek a fenyegetések előrejelzését, a károk megelőzését és az emberek védelmét segítik. Mindezt minden szinten a társadalom egészére kiterjedő megközelítésbe ágyazva fogja megvalósítani.

Az egészségügyi ágazat számos szervezetet és szereplőt jelent, többek között kórházakat, klinikákat, gondozóotthonokat, rehabilitációs központokat és különböző egészségügyi szolgáltatókat, továbbá a gyógyszeripart, a gyógyászati és biotechnológiai ipart, az orvostechnikai eszközök gyártóit és az egészségügyi kutatóintézeteket. Ez a cselekvési terv elsősorban a kórházak és az egészségügyi szolgáltatók kiberbiztonságára összpontosít, azaz valamennyi olyan természetes vagy jogi személy – vagy bármely más szervezet – védelmére, aki vagy amely jogszerűen nyújt egészségügyi ellátást egy tagállam területén[3]. A kórházak és az egészségügyi szolgáltatók állnak legszorosabb kapcsolatban az emberekkel, és szorosan együttműködnek más egészségügyi szervezetekkel. A kórházak és az egészségügyi szolgáltatók kiberbiztonságának megerősítésére irányuló intézkedéseknek ugyanakkor ki kell terjedniük a tágabb ellátási láncot és ökoszisztémát érintő azon kockázatokra is, amelyek például olyan szervezetektől erednek, amelyek az egészségügyi adatokat kutatás vagy gépi tanulás céljára használják fel, vagy orvostechnikai eszközöket, kiváltképpen digitalizált orvostechnikai eszközöket gyártanak, amelyek az internethez vagy más eszközökhöz vannak csatlakoztatva (a továbbiakban: a dolgok internete).

Bár az egészségügyi rendszerek biztonságos működtetése elsősorban nemzeti hatáskörbe tartozik, az egészségügy az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló NIS 2 irányelv[4] értelmében is kritikus ágazatnak minősül. A kiberbűnözők és más fenyegető szereplők határokon átnyúlóan működnek, vagyis az egészségügyi szervezetek hasonló kiberbiztonsági kihívásokkal szembesülnek valamennyi tagállamban. Az európai szintű együttműködésnek köszönhetően megoszthatók és kiterjeszthetők a legjobb uniós és nemzeti szintű gyakorlatok. A cselekvési terv ezért uniós szintű koordinációt és intézkedéseket javasol, egyben pedig felszólítja a tagállamokat is, hogy tegyenek lépéseket az egészségügyi ellátás és a tágabb értelemben vett egészségügyi ökoszisztéma javítása érdekében.

Mivel a legjobb gyógyszer a megelőzés, a cselekvési terv középpontjában első helyen az ágazat kiberbiztonsági incidensek **megelőzésére** irányuló kapacitásainak kiépítése áll. Másodsorban, a cselekvési terv részletes intézkedéseket határoz meg a kiberbiztonsági információmegosztás és a

[3]A határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről szóló 2011/24/EU európai parlamenti és tanácsi irányelv 3. cikkének g) pontja https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32011L0024.
[4]Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2 irányelv); https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:02022L2555-20221227.

kiberfenyegetések **észlelését** célzó képesség javítására, amely a gyorsabb reagálást teszi lehetővé. Harmadszor, olyan intézkedéseket ír elő, melyek segítik az incidensekre való jobb **reagálást** és a működés azt követő **helyreállítását**. Végezetül a cselekvési terv felvázolja, hogy miként lehet visszatartani a kibertámadással fenyegető szereplőket attól, hogy európai egészségügyi rendszereket válasszanak célpontjuknak.

A cselekvési terv végrehajtása az egészségügyi szolgáltatókkal, a tágabb értelemben vett egészségügyi ökoszisztéma tagjaival, valamint a tagállamokkal és a kiberbiztonsági közösséggel együtt történik majd. Az együttműködésen alapuló megközelítés kulcsfontosságú ahhoz, hogy meg lehessen határozni a leghatásosabb további intézkedéseket és finomhangolni lehessen őket, hogy a megközelítés Európa valamennyi kritikus egészségügyi szolgáltatójának javára váljon. Ezért a közleményhez számos átfogó konzultáció fog kapcsolódni, az érdekelt felek, az ipar és a tagállamok szempontjainak figyelembevétele érdekében.A kiberfenyegetések határok nélküli és összekapcsolt jellege miatt a kiberbiztonsághoz elengedhetetlen a nemzetközi együttműködés. Hasonló kiberfenyegetések jellemzők a bővítési és a szomszédos országokban, valamint az Unió más stratégiai partnerországaiban is. Ezek végső soron az EU kritikus infrastruktúrájának biztonságát is veszélyeztethetik. Ezért fontos, hogy a cselekvési terv végrehajtásából levont tanulságokat az Unió és a bővítési és más partnerországok közötti együttműködés során is figyelembe vegyük, az adott országok fenyegetettségi szintjéhez mérten.

## 2. A kórházak és az egészségügyi szolgáltatók előtt álló kiberbiztonsági kihívások

*Az egészségügyi ágazatot érintő kiberfenyegetések*

A kibertámadások egyre gyakoribbak lettek mind világszerte, mind pedig az Unión belül, egyre összetettebb és dinamikusabb fenyegetettségi helyzetet rajzolva ki. A mesterséges intelligencia fejlődésének következtében a bűnözők és a rossz szándékú szereplők még hatékonyabb, nagyobb műveleti pontosságú és kiterjedtebb hatást kiváltani képes eszközökkel rendelkeznek, ugyanakkor változott a kibervédelmi lehetőségek tárháza is, és lehetővé vált az automatizált, valós idejű fellépés a támadásokkal szemben.

A zsarolóvírusok továbbra is kritikus kiberbiztonsági kihívást jelentenek az EU-ban és világszerte; egy jelentés szerint 2031-ig az ezekkel kapcsolatos éves költségek meghaladhatják a 250 milliárd EUR-t globális szinten[5]. A zsarolóvírusos támadás során a bűnözők nemcsak titkosítják az áldozatok adatait, hogy váltságdíjat kérjenek fejükben, hanem egyre gyakrabban érzékeny információkat is kiszivárogtatnak további nyomásgyakorlásként. Komoly kihívást jelent emellett a szoftverek és hardverek sérülékenysége is. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA)[6] szerint az

[5] Cybersecurity Ventures (2024. június 1.): „A zsarolóvírusok okozta kár várhatóan a 265 milliárd USD dollárt is túl fogja lépni 2031-re világviszonylatban". Elérhető az alábbi internetes oldalon:https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6]Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint

egészségügyi ágazattól érkezett a legtöbb olyan bejelentés biztonsági incidensekről, amelyek hardver- vagy szoftver-sérülékenységekhez kapcsolódtak[7]. Növekvő számban fordulnak elő továbbá elosztott szolgáltatásmegtagadási támadások (DDoS-támadások), amelyek a megcélzott rendszert olyan mértékű adatforgalommal terhelik, hogy az elérhetetlenné válik a jogszerű felhasználók számára[8].

Az egészségügyi ágazat hasonló kiberfenyegetettségi tendenciákkal szembesül, melyek hangsúlyosan zsarolóvírus-támadások formájában jelentkeznek. Az ENISA szerint 2021 és 2023 között az egészségügyi ágazatot ért elemzett kiberbiztonsági incidensek 54 %-át zsarolóvírusok okozták. A támadások 83 %-a anyagi indíttatású volt, köszönhetően annak, hogy az egészségügyi adatok igen értékesek, míg 10 %-uk hátterében ideológiai szándék állt[9]. Hasonlóképpen, a Bizottság 2024. évi jelentése megállapította, hogy a betegellátásra hatást gyakorló – például késedelmes kezelést vagy diagnózist eredményező, vagy a készenléti segélyszolgálat rendelkezésre állását gátló – támadások 71 %-a zsarolóvírus-típusú volt[10]. A zsarolóvírus-támadások különösen nagy mértékben megzavarhatják az egészségügyi szolgáltatások nyújtását, veszélyeztetve a betegek biztonságát. Ezenkívül a zsarolóvírus-támadások gyakran a betegek adatainak, köztük gyakran érzékeny egészségügyi adatoknak a megsértésével járnak[11], és sértik az embereknek a személyes adatok védelméhez való alapvető jogát.

Az egészségügyi ellátás fokozódó digitalizációjával egyben a támadási felület is növekszik. A digitális évtized helyzetéről szóló 2024. évi jelentés megállapítja, hogy az alapellátásban az uniós polgárok átlag 79 %-a rendelkezik online hozzáféréssel elektronikus egészségügyi dokumentációjához[12]. Az elektronikus egészségügyi dokumentációk, a klinikai információs rendszerek, a kórházi munkafolyamatokat biztosító rendszerek, a kezelések visszatérítésére használt informatikai rendszerek, az orvosi képalkotó rendszerek és a diagnosztikai vagy betegfelügyeleti célú orvostechnikai eszközök mind olyan digitális eszközök, amelyek jelentős szerepet játszhatnak az egészségügyi ágazat hatékonyságának és teljesítményének növelésében, de ezek egyben a kiberbiztonsági támadások potenciális célpontjai is. Egyes egészségügyi tevékenységek, például az intenzív ellátás vagy a radiológiai képalkotás, illetve bizonyos orvosi szakterületek, mint pl. az onkológia vagy a kardiológia, amelyek nagymértékben a digitális eszközöktől függenek, fokozottan ki vannak téve a kibertámadások kockázatának. Emellett az ellátási lánc akadozása miatt előfordulhat, hogy olyan eszközöket kell beszerezni, melyek kiberbiztonsága nem elégséges, ami tovább növeli a meglévő általános kockázatokat.

---

az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály).https://eur-lex.europa.eu/eli/reg/2019/881/oj?eliuri=eli%3Areg%3A2019%3A881%3Aoj&locale=hu.

[7] Az ENISA fenyegetettségi helyzetjelentése: Egészségügyi ágazat (2023. július).

[8] Az ENISA fenyegetettségi helyzetjelentése, 2024.

[9] Az ENISA fenyegetettségi helyzetjelentése: Egészségügyi ágazat (2023. július). A jelentés elemzett egészségügyi szolgáltatókat és más típusú szervezeteket, köztük olyanokat, amelyek egészségügyi kutatást végeznek, de bizonyos egészségügyi termékek gyártóit is, valamint egészségügyi hatóságokat, egészségbiztosítási szervezeteket, valamint bentlakásos kezelőlétesítményeket és szociális szolgáltatókat. Elérhető a következő címen:https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Európai Bizottság: Közös Kutatóközpont, Reina, V. és Griesinger, C., Cyber security in the health and medicine sector – A study on available evidence of patients health consequences from cyber incidents in healthcare settings, az Európai Unió Kiadóhivatala, 2024., https://data.europa.eu/doi/10.2760/693487.

[11] Az ENISA egészségügyi ágazatra vonatkozó fenyegetettségi helyzetjelentése szerint az elemzett zsarolóvíruss-incidensek 43 %-ában megerősítették, hogy adatvédelmi incidens, illetve adatlopás történt.

[12] A digitális évtized helyzetéről szóló 2024. évi jelentés.

A Covid19-világjárvány idején egy zsarolóvírusos támadás például nagyrészt megbénította az ír egészségügyi rendszert, minek következtében a sürgősségi ellátást nyújtó 54 kórházból 31-ben le kellett mondani minimum néhány szolgáltatást az incidens reggelén[13]. Az egészségügyi szolgálatoknak vissza kellett térniük a papíralapú nyilvántartásra, ami lassította a műveletek hatékonyságát. A támadás forrása egy adathalász e-mail csatolmánya volt[14]. Az incidens rámutatott arra, hogy milyen nagy hatása lehet a különböző rendszereken keresztül terjedő kibertámadásoknak, és következésképpen arra, hogy milyen fontos, hogy az egészségügyi szervezetek jelentette támadási felületet teljeskörűen védjük. Világossá tette továbbá, hogy a kiberhigiéniai és kiberbiztonsági kultúra megteremtése a szervezetek egészében alapvetően fontos.

*A kórházak és az egészségügyi szolgáltatók kiberbiztonsági érettsége*

Az egészségügyi ellátás nagyon változatos képet mutat az Unióban, a kórházak és az egyéb egészségügyi szolgáltatók tulajdonosi összetétele, szerkezete és a mérete tagállamonként igen eltérő. Az egészségügy irányítása néhol nemzeti szintű, központosított megközelítésen alapul, másutt regionális vagy helyi szinten szerveződik; az egészségügyi szolgáltatók van ahol állami, van ahol magántulajdonban vannak. Emellett előfordulhat, hogy akár egy adott országon belül is különbségek tapasztalhatók, például ha jelentős társadalmi-gazdasági és területi különbségek vannak a régiók között – a kép tehát igen összetett. Egy ilyen összetett egészségügyi környezetben kihívást jelenthet kezelni a fertőző betegségek miatt kialakult jelentős egészségügyi válságokat, mint például a Covid19-világjárványt, de az éghajlatváltozással kapcsolatos egészségügyi kockázatokat is. Végezetül jelentős különbségek és széttöredezettség figyelhető meg a digitalizáltság fokában és abban, hogy az egészségügyi szolgáltatók milyen mértékben adaptálják a technológiákat. A helyzet összetettségét jól példázza, hogy egy kiberbiztonsági incidens okozta szolgáltatáskiesés súlyos károkat okozhat kisebb egészségügyi létesítmények betegeinek is, legyen szó akár klinikákról, akár olyan sürgősségi orvosi szolgáltatásokról, amelyek viszonylag kevesek számára nyújtanak alapvető szolgáltatást.

Az Unió kiberbiztonságának helyzetéről szóló 2024. évi ENISA-jelentés[15] szerint az uniós egészségügyi ágazat kiberbiztonsági érettsége mérsékelt, és Európa-szerte jelentős különbségek vannak az egészségügyi szervezetek kiberbiztonsági érettségének szintje között. Sok kulcsfontosságú területen számos hiányosság figyelhető meg. Olyan kérdések tartoznak ide többek között, hogy rendelkezésre áll-e kellő emberi erőforrás, megfelelő ismerettel rendelkeznek-e a szervezetek az információs és kommunikációs technológiai (IKT) ellátási láncokról, valamint hogy a termékek el vannak-e látva korszerű biztonsági funkciókkal. Az ágazat számára nehézséget okoznak az alapvető kiberhigiéniai és nélkülözhetetlen biztonsági intézkedések, amit jól illusztrál az a tény is, hogy szinte minden

[13]Ír egészségügyi hivatal (2021): „Conti cyber attack on the HSE: Independent Post Incident Review”.
[14]Ír egészségügyi hivatal: „Cyber-attack and HSE response”. Elérhető a következő internetes oldalon:https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA: az Unió kiberbiztonságának helyzetéről szóló 2024. évi jelentés (2024. szeptember). Elérhető a következő címen:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

megkérdezett egészségügyi szervezet számára kihívást jelent a kiberbiztonsági kockázatértékelések elvégzése, és a szervezetek közel fele még sosem végzett kockázatelemzést[16].

A kórházak kiberbiztonsága terén jelentős kihívás, hogy az információs technológia és az operatív technológia átfedi egymást, és metszetükben különböző biztonsági prioritások találkoznak a titoktartás, rendelkezésre állás és a megbízhatóság terén, és az egyik területen felmerülő problémák hatással lehetnek a másikra. Az Unió kiberbiztonságának helyzetéről szóló 2024. évi ENISA-jelentés hangsúlyozza továbbá, hogy az egészségügyi ágazat az egészségügyi szervezetek, eszközök és termékek sokfélesége miatt nem képes kellőképpen garantálni az ágazati IKT-termékek és -folyamatok biztonságát.

Ez a sokféleség, valamint az egyes kórházak személyzetének és vezetőségének eltérő mértékű kibertudatossága együttesen összetett kihívást jelentenek az egészségügyi rendszerek kiberbiztonságának garantálása szempontjából. Ezt példázza, hogy a kiberkészségekről szóló 2024. évi Eurobarométer felmérés szerint az egészségügyi, oktatási és szociális ellátási ágazatban a megkérdezett vállalatoknak csak 25 %-a nyújtott kiberbiztonsági képzést vagy tájékoztatást a felmérést megelőző 12 hónapban[17]. Ezért lépni kell, és erősíteni kell a kibertudatosság kultúráját az első vonalban dolgozó egészségügyi szakemberek körében. Az egészségügyi szolgáltatók kiberbiztonságának sérülékenységét növeli például a személyzet rotációja, a munkaállomások közös használata, a nem megfelelő hitelesítési mechanizmusok és az eltávolítható adathordozók használata[18].

Az információs technológiát és az operatív technológiát sok esetben legalább részben kiszervezik. A 2024. évi Eurobarométer felmérés megállapította, hogy az egészségügyi, az oktatási és a szociális ellátási ágazatban a legmagasabb azon vállalatok aránya (57 %), amelyek legalább néhány kiberbiztonsági részfeladatot kiszerveznek[19]. Kifejezett tendencia figyelhető meg a felhőalapú számítástechnikára való átállás terén, melyet a méretezhető adattárolás és -kezelés, a költséghatékonyság, a hatékonyabb együttműködés igénye és az olyan fejlett technológiák támogatásának szüksége vezérel, mint a mesterséges intelligencia vagy az orvosi dolgok internete. 2022-ben az egészségügyi szervezetek 58 %-a használt felhőalapú digitális egészségügyi platformot[20]. A váltás ugyan jelentős hatékonyságnöveléssel járhat, ugyanakkor kockázatokat is rejt, amelyek kezeléséhez megalapozott döntések szükségesek a beszerzéssel és a konfiguráció biztonságosságával kapcsolatban.

E kihívások mindegyikéhez hozzájön a kapacitásépítés és a finanszírozás kérdése is. A kiberbiztonság finanszírozása korlátozott mértékű az egészségügyi ágazatban, és továbbra is általános kihívást jelent az

[16] Az ENISA fenyegetettségi helyzetjelentése: Egészségügyi ágazat (2023. július). Elérhető a következő címen:https://www.enisa.europa.eu/publications/health-threat-landscape.

[17]547. sz. Eurobarométer gyorsfelmérés a kiberkészségekről (2024. május). Elérhető online a következő helyen:https://europa.eu/eurobarometer/surveys/detail/3176.

[18] Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.

[19]547. sz. Eurobarométer gyorsfelmérés a kiberkészségekről (2024. május). Elérhető online a következő helyen:https://europa.eu/eurobarometer/surveys/detail/3176.

[20] ENISA: 2022. évi NIS beruházási jelentés (2022. november). Elérhető a következő címen:https://www.enisa.europa.eu/publications/nis-investments-2022.

egész Unióban[21]. Ehhez járul még az is, hogy az említett finanszírozási kihívásokat úgy kell megoldani, hogy a háttérben a népességöregedés várhatóan szintén nagy nyomást fog gyakorolni az európai egészségügyi rendszerek költségvetésére a következő évtizedekben.

Azok a problémák, hogy továbbra is használatban vannak elavult eszközök és régről örökölt rendszerek, hogy korlátozott forrásokkal kell megelőzni az incidenseket, illetve reagálni rájuk, és a kiberbiztonsági érettség nem megfelelő, gyakran finanszírozási hiányokra vezethetők vissza. A kórházak számára folyamatos kihívást jelent, hogy egyensúlyt teremtsenek a biztonságos és digitális infrastruktúra és a betegellátás javításához szükséges egyéb olyan beruházások között, mint például orvosok és más egészségügyi szakemberek felvétele, új diagnosztikai és kezelési módszerek bevezetése, valamint eszközbeszerzés. Az ENISA[22] adatai szerint a 12 vizsgált ágazatból az egészségügyi ágazat csak 7. helyen áll az információbiztonsági kiadásoknak az összes informatikai kiadáson belüli arányát tekintve; az egészségügyi ágazatban a medián érték 8,3 %.

## 3. Kórházak és Egészségügyi Szolgáltatók Európai Kiberbiztonsági Támogató Központja

Az uniós kiberbiztonsági keret számtalan eszközt kínál a kórházak és az egészségügyi szolgáltatók biztonságának és rezilienciájának javítására. A fent kiemelt megannyi kihívás kezelésére egységes stratégiai megközelítést kell kidolgozni uniós szinten, amely összefogja a kiberfenyegetések hatékony kezeléséhez szükséges erőforrásokat, szakértelmet és eszközöket. Az átfogó áttekintés, valamint a jobb tervezés és koordináció elengedhetetlen ahhoz, hogy az Unió egészében segíteni tudjuk az egészségügyi szolgáltatókat a jobb védekezésben. Az EU kritikus infrastruktúrájának védelmére és támogatására vonatkozó megbízatásának[23] részeként az ENISA a legalkalmasabb arra, hogy erre a célra szervezetén belül létrehozza **a Kórházak és Egészségügyi Szolgáltatók Európai Kiberbiztonsági Támogató Központját**[24].

A Támogató Központnak fokozatosan **ki kell dolgoznia egy, a kórházak és az egészségügyi szolgáltatók igényeire szabott átfogó szolgáltatáskatalógust**, amely felvázolja a felkészültség, a megelőzés, az észlelés és a reagálás terén rendelkezésre álló szolgáltatások körét. A Támogató Központnak a tagállami hatóságokkal együttműködve, valamint a kórházak és az egészségügyi szolgáltatók tapasztalataira építve egy felhasználóbarát és könnyen hozzáférhető adattárat kell létrehoznia az összes rendelkezésre álló európai, nemzeti és regionális szintű eszközről. Tevékenységei gyakorlásakor biztosítania kell a tagállamokkal a megfelelő koordinációt, és támogatnia kell az intézkedések szükség szerinti, valós idejű rangsorolását és végrehajtását.

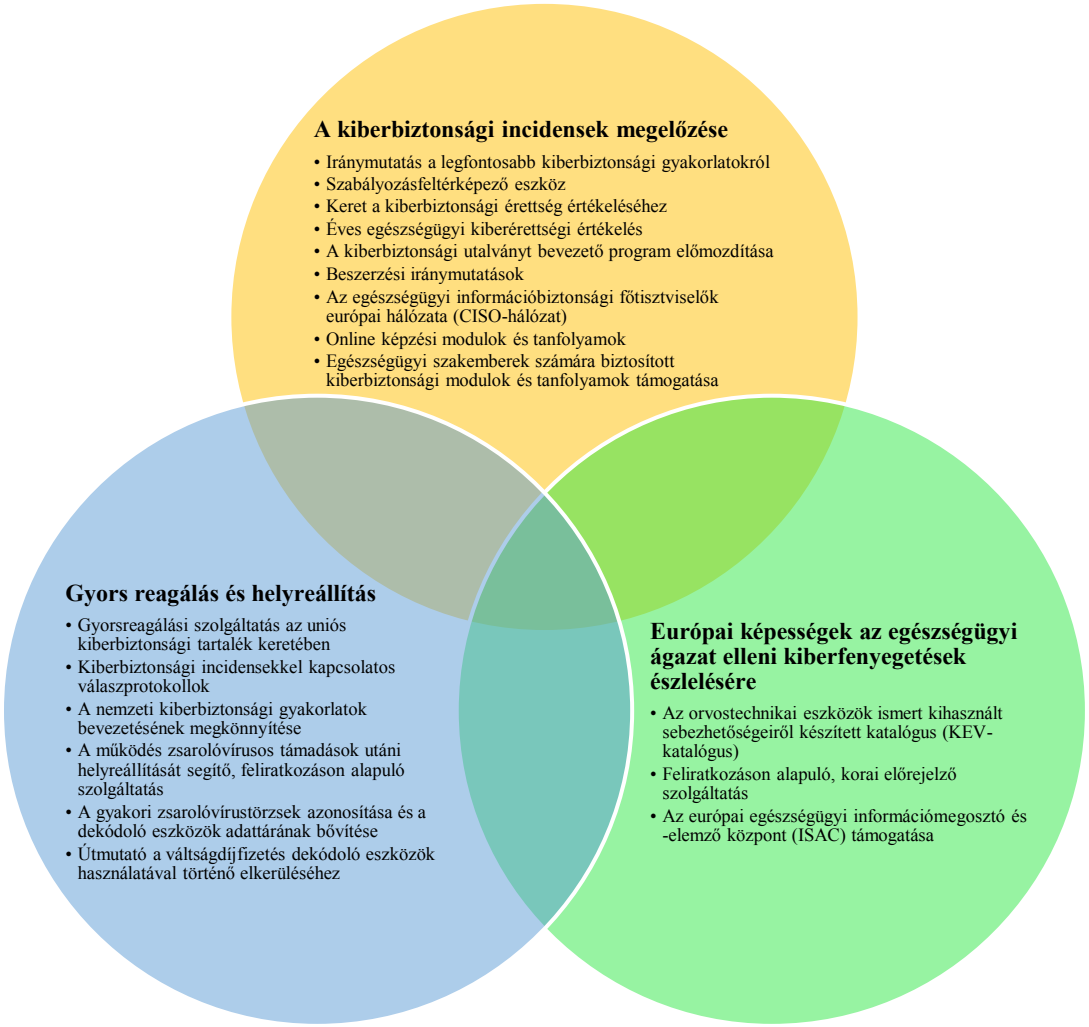
[21]Az egészségügyi szolgáltatások és az orvosi ellátás megszervezése és biztosítása az Európai Unió működéséről szóló szerződés 168. cikke értelmében nemzeti hatáskörbe tartozik, és az egészségügyi rendszerek finanszírozása tagállamonként eltérő.

[22] ENISA: 2022. évi NIS beruházási jelentés (2022. november). Elérhető a következő címen:https://www.enisa.europa.eu/publications/nis-investments-2022.

[23]Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

[24] Ez a dokumentum a „Támogató Központ” kifejezést szinonimaként használja.

Annak érdekében, hogy a Támogató Központ szolgáltatáskatalógusának kidolgozásához megfelelő építőkövek álljanak rendelkezésre, a Bizottság kísérleti projektek indítását fogja javasolni Unió-szerte. Ezek a projektek a legjobb kiberhigiéniai és -biztonsági kockázatértékelési gyakorlatok kidolgozására fognak irányulni, valamint eleget kívánnak tenni a folyamatos kiberbiztonsági nyomon követés, a fenyegetésekkel kapcsolatos hírszerzés és a biztonsági incidensekre való reagálás iránti igénynek, a legkorszerűbb kiberbiztonsági megoldásokat használva. E kísérleti projekteket az Európai Kiberbiztonsági Kompetenciaközpont (ECCC) által végrehajtott Digitális Európa program fogja finanszírozni, és az eredmények további uniós szintű intézkedéshez, ezen belül a Támogató Központ munkájához fognak alapul szolgálni.



1. ábra: A Támogató Központ kórházakra és egészségügyi szolgáltatókra vonatkozó szolgáltatáskatalógusának koncepciói

### *3.1. A kiberbiztonsági incidensek megelőzése*

*Egyszerű intézkedések az incidensek előfordulási esélyének csökkentésére*

Egy becslés szerint olyan alapvető kiberbiztonsági intézkedésekkel, mint a rendszerek naprakészen tartásával, biztonsági mentésekkel, valamint többtényezős hitelesítés alkalmazásával a szervezeteket érő támadások 98 %-a kivédhető[25]. A leghatásosabb kiberhigiéniai és kockázatkezelési intézkedések közül sok rendkívül kézenfekvő, és viszonylag egyszerűen kivitelezhető, tehát a kiberbiztonságot kis ráfordítással nagyban javítaná. A Támogató Központnak ezért egyik kulcsfontosságú feladataként **egyértelmű, célzott iránymutatást kell kidolgoznia, amely kiemeli a legfontosabb kiberbiztonsági gyakorlatokat, és segíti az egészségügyi szolgáltatókat a végrehajtásukban**. Ez a támogatás nem korlátozódhat a nagy kórházakra, hanem személyre szabott tanácsadásban kell részesíteni a kisebb szervezeteket is, mint pl. a helyi háziorvosi rendelőket és szakklinikákat, amelyeknek gyakran nincs kellő erőforrásuk ahhoz, hogy specializált kiberbiztonsági csoportokhoz forduljanak, de a kibertámadásoknak ugyanúgy ki vannak téve. Figyelembe kell venni továbbá az egyes egészségügyi szervezetek regionális jelentőségét a betegellátás biztosításában, például a ritkán lakott területeket tekintve. A sok érzékeny személyes adatot kezelő egészségügyi kutatóintézeteknek szintén hasznukra válhat, ha iránymutatást kapnának azokról az alapvető kiberbiztonsági intézkedésekről, amelyek fokozhatják rezilienciájukat.

Az egészségügyi szervezeteknek az uniós jogszabályokból fakadóan számos kiberbiztonsági kötelezettségnek eleget kell tenniük[26]. Bár e kötelezettségek alapvetőek annak biztosításához, hogy a

[25] Microsoft Digital Defense Report (A Microsoft digitális védelemre vonatkozó jelentése), 2022. Elérhető a következő címen:https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26]Például a NIS 2 irányelv; az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről (a kiberrezilienciáról szóló rendelet), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32024R2847&qid=1737711465680; az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechnikai eszközökről https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A02017R0745-20250110&qid=1737711549642 (az orvostechnikai eszközökről szóló rendelet); az Európai Parlament és a Tanács (EU) 2017/746 rendelete (2017. április 5.) az *in vitro* diagnosztikai orvostechnikai eszközökről (az *in vitro* diagnosztikai orvostechnikai eszközökről szóló rendelet); https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A02017R0746-20250110&qid=1737711783052; az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679; az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (a mesterséges intelligenciáról szóló rendelet), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1689; az európai egészségügyi adattérről szóló európai parlamenti és tanácsi rendeletre irányuló javaslat, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A52022PC0197. A tárgyalások 2024 tavaszán politikai megállapodással lezárultak. A véglegesítést követően a szöveget várhatóan 2025 tavaszán teszik közzé a Hivatalos Lapban.

kiber- és adatbiztonság szilárd közös alapokon álljon, a szabályozási környezet nem lehet szükségtelenül bonyolult és nehezen alkalmazható. A jogszabályi megfelelésre koncentrálva nem téveszthetjük szem elől a fő célkitűzést, ami a megbízható kiberbiztonsági kultúra előmozdítása. Egy **könnyen hozzáférhető szabályozásfeltérképező eszköz segíthet csökkenteni azon szervezetek adminisztratív terheit, amelyek egyszerre több szabályozási eszköz hatálya alá tartoznak**. Az iránymutatások és az eszköztárak kidolgozása mellett a Támogató Központnak szorosan együtt kell működnie a Bizottsággal és a tagállamokkal, hogy ezt a szabályozásfeltérképező eszközt mielőbb létrehozza és elterjessze. A Támogató Központnak tehát fontos szerepe lenne abban, hogy a kiberbiztonsági szabályok könnyen érthetők és végrehajthatók legyenek, például azáltal, hogy végrehajtási iránymutatást[27] nyújt, és szükség esetén támogatja a vonatkozó szabványozási munkát.

A helyes kiberhigiéniai gyakorlatok egyszerű megvalósításának eszközeként fognak szolgálni a közeljövőben az **európai digitális személyiadat-tárcák** is. Az egészségügyi adatokhoz való jogosulatlan hozzáférés kockázatának csökkentéséhez elengedhetetlen, hogy az azonosítási mechanizmusoknál ne olyan gyenge védelmet biztosító megoldásokra támaszkodjunk, mint a jelszavak. Döntő, hogy elmozduljunk a megbízható azonosításon alapuló biztonságos bejelentkezési megoldások felé. Az európai digitális személyiadat-tárca harmonizált, uniós szintű megközelítést kínál az egészségügyi szakemberek elektronikus azonosítására, és 2026 végétől szilárd és egységes megoldást fog kínálni. 2027 végétől valamennyi online egészségügyi információs rendszernek erős felhasználói hitelesítést kell alkalmaznia, és ennek során kötelező elfogadniuk az európai digitális személyiadat-tárcát azonosítási célokra[28].

*Felkészültség és célzott támogatás*

A hatékony kiberbiztonság sarokkövét képezi a készültségi tesztelés, amely olyan intézkedéseket foglal magában, mint a behatolási tesztelés, ezért a Bizottság már elkülönített az ENISA számára forrásokat a készültségre vonatkozó kísérleti kezdeményezések megvalósítására. Ezek feltárták, hogy az egészségügyi ágazat egyike azon területeknek, ahol fokozott tesztelésre és a további értékelésekre van szükség annak megállapítása érdekében, hogy miképp fokozható a kiberbiztonsági érettség. A kiberszolidaritásról szóló jogszabály hatálybalépésével ezek az erőfeszítések jelentősen fokozódni fognak, és ebben az ECCC-nek vezető szerepet fog jutni. Ezen igény kezelése érdekében a Bizottság – a Kiberbiztonsági Együttműködési Csoporttal, az EU-CyCLONe-nal[29] és az ENISA-val konzultálva – javaslatot fog tenni arra, hogy az egészségügyet sorolják azon ágazatok közé, amelyek a kiberszolidaritásról szóló jogszabály keretében támogatást kaphatnak **összehangolt felkészültségi tesztelésre**. Ezenkívül a Támogató Központnak **kifejezetten az egészségügyre vonatkozóan testre szabott keretet kell kidolgoznia a kiberbiztonsági érettségi értékelésekhez**. A kiberbiztonsági érettségi értékelések megvilágítanák a szervezetek számára sérülékenységeiket, és egyben lehetővé tennék, hogy demonstrálják a betegek és az érdekelt felek számára kiberbiztonsági felkészültségüket,

[27] Az általános adatvédelmi rendelet értelmezésére vonatkozó iránymutatások kidolgozása az Európai Adatvédelmi Testület (EDPB) hatáskörébe tartozik. Az ENISA iránymutatásának kidolgozása során teljes mértékben tiszteletben kell tartani az Európai Adatvédelmi Testület előjogait.
[28] Az (EU) 910/2014 rendelet 5f. cikkének (1) és (2) bekezdése.
[29] Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata.

növelve ezáltal a szolgáltatásaikba vetett bizalmat. A Támogató Központnak egy átfogó, **éves egészségügyi kiberérettségi értékelést** kellene végeznie, amely egyértelmű áttekintést nyújtana az egészségügyi ágazat kiberbiztonságáról nemzeti és uniós szinten egyaránt.

Az egészségügyi ágazat nagymértékben támaszkodik külső szerződő felekre a kiberbiztonsági szolgáltatásokat illetően[30], ami rávilágít arra, hogy a védekezés megerősítéséhez célzott támogatásra van szükség. A sikeres kezdeményezésekre, például az uniós innovációs utalványokra építve **a tagállamoknak célirányos intézkedéseket kell hozniuk; ilyen lehet például a mikro-, kis- és közepes méretű kórházak és egészségügyi szolgáltatók számára biztosított kiberbiztonsági utalványok bevezetése**. Az utalványok pénzügyi támogatást biztosítanának konkrét kiberbiztonsági intézkedések bevezetéséhez. Az utalványokat a felkészültségi tesztelés és az érettségi értékelések megállapításainak figyelembevételével kialakított rangsor alapján lehetne kiosztani.

Az utalványok vagy más támogatási programok hatékony bevezetéséhez alapvetően fontos a helyi ismeretek és az adottságok feltérképezése, mert csak így biztosítható az intézkedések relevanciája és hozzáférhetősége. Az uniós alapokból, köztük az Európai Regionális Fejlesztési Alapból már most is aktívan támogatják a kiberbiztonsági és digitális egészségügyi kezdeményezéseket. Ezek ezért eszközül szolgálhatnak az egészségügyi szolgáltatók számára nyújtandó célzott kiberbiztonsági utalványrendszer kidolgozásához. Az ezirányú munka előmozdítása érdekében célszerű, ha a Támogató Központ a tagállamokkal és a regionális programhatóságokkal együttműködve hozzájárul a szóban forgó regionális utalványrendszerek kidolgozásához, minek során figyelembe kell venni a már meglévő nemzeti projektek, valamint a Digitális Európa program keretében finanszírozott intézkedések tanulságait, ezzel biztosítva a célszerű és hatásos végrehajtást.

Emellett a Horizont programok 2014 óta fontos szerepet játszanak számos olyan kutatási kezdeményezés finanszírozásában, amelyek az egészségügyi intézmények, például a kórházak kiberfenyegetésekkel szembeni rezilienciájának fokozására és a kialakulóban lévő technológiákkal kapcsolatos visszaélések kockázatának csökkentésére irányulnak. Ezek eredményeként egy sor speciális eszköz, keret és rendszer áll rendelkezésre, például kockázatértékelési eszközök, a személyes adatok védelmét biztosító adatmegosztó platformok, kriptográfiai megoldások, kibertudatossági képzési programok és valós idejű fenyegetésészlelő rendszerek. Az említett megoldásokat szigorúan validálták, valós egészségügyi környezetben kipróbálva őket, hogy ténylegesen megbizonyosodjanak hatékonyságukról és gyakorlati alkalmazhatóságukról a kiberfenyegetésekkel szemben.

*Az egészségügyi ellátási láncok biztosítása*

Az egészségügyi szervezetek számára az egyik legfontosabb kihívást az összetett IKT-ellátási láncok irányítása jelenti, amelyek sokféle termékre kiterjednek, például az internetre csatlakoztatott orvostechnikai eszközökre, az elektronikus egészségügyi nyilvántartási rendszerekre és az irodai hardverekre. A kórházaknak és az egészségügyi szolgáltatóknak megbízható és biztonságos IKT-rendszerekre és -szolgáltatásokra van szükségük a működésükhöz. Az egészségügyi ágazatot érintő

[30]Lásd az ENISA hálózat- és információbiztonsági beruházásokról szóló 2023. évi jelentését (2023. november), amely kiemeli a kiberbiztonsági ellenőrzéshez és megfeleléshez nyújtott külső támogatás fontosságát. Elérhető a következő címen:https://www.enisa.europa.eu/publications/nis-investments-2023.

kiberbiztonsági kihívások kezelése érdekében a Kiberbiztonsági Együttműködési Csoportnak **összehangolt biztonsági kockázatértékelést kell végeznie, amelynek keretében az orvostechnikai eszközök ellátási láncaival kapcsolatos technikai és stratégiai kockázatokat is értékeli, valamint kockázatcsökkentő intézkedéseket javasol**[31]. Adott esetben a Kiberbiztonsági Együttműködési Csoportnak együtt kell működnie az orvostechnikai eszközökkel foglalkozó koordinációs csoporttal.

A kiberrezilienciáról szóló jogszabály új, átfogó keretbe foglalja azokat a kiberbiztonsági követelményeket, amelyek szinte valamennyi hardver- és szoftvertermék tervezésére, kialakítására és fejlesztésére vonatkoznak – ideértve az aktívan kihasznált sérülékenységek kezelését, javítását és bejelentését is –, az értéklánc valamennyi szakaszában[32]. Az orvostechnikai eszközöket mint terméktípust a társadalom számára leginkább érzékeny területek egyikén használják fel. Az ilyen termékekre vonatkozó kiberbiztonsági követelmények az orvostechnikai eszközökről szóló, már meglévő rendeletből és az in vitro diagnosztikai orvostechnikai eszközökről szóló rendeletből erednek[33]. Az említett rendeletek folyamatban lévő értékelése a szóban forgó keretek közötti fokozott koherencia és a szinergiák lehetőségét vizsgálja, az egyszerűsítés és a korszerű kiberbiztonsági megoldások érdekében.

A kockázatértékelés megállapításai támogatást nyújthatnak az egészségügyi szervezetek számára, amikor azok a NIS 2 irányelvben előírtak szerint felülvizsgálják az ellátási láncaik kiberbiztonsági gyakorlatait, valamint új **közbeszerzési iránymutatások**[34] kidolgozásának alapját is képezhetik. Az ENISA Támogató Központja által kidolgozott iránymutatásoknak tükrözniük kell a közelmúlt tendenciáit, például a betegadatok felhőben történő tárolásának elterjedését, beleértve azt is, hogy az elektronikus egészségügyi adatokat biztonságos módon kell a felhőalapú környezetbe migrálni. Az új iránymutatásoknak továbbá gyakorlati eszközöket kell kínálniuk a szervezetek számára az ellátási láncok nyomon követéséhez, beleértve az irányított biztonsági szolgáltatókat, a tanúsítási jelentéseket vagy a harmadik féltől eredő kockázatok értékelését is.

A felhőalapú adattárolás tekintetében további intézkedésekre van szükség az érzékeny egészségügyi adatok kezelésével kapcsolatos különleges kihívások kezelése érdekében, beleértve a fokozott biztonsági, adatvédelmi és működési kockázatokat. A biztosítékok megerősítése érdekében a szakértők azt javasolják, hogy a felhőszolgáltatásokat „alapértelmezett és beépített biztonság” jellemezze. Ez a megközelítés a biztonságos infrastruktúrára, a proaktív sérülékenység-menedzsmentre, valamint a kormányzati és magánkézben lévő felhőmegoldások kombinációjára helyezi a hangsúlyt. A folyamatos nyomon követés és a szolgáltatóspecifikus tanúsítványok – például a biztonságszolgáltatói tanúsítások,

[31]A NIS 2 irányelv 22. cikke szerint.

[32]Első lépésként 2025. augusztus 1-jétől kezdve az olyan rádióberendezések tág kategóriáinak, amelyek nem tartoznak sem az orvostechnikai eszközökről szóló rendelet, sem az in vitro diagnosztikai orvostechnikai eszközökről szóló rendelet hatálya alá, az egységes piacon történő forgalomba hozatalukkor kell majd megfelelniük a rádióberendezésekről szóló irányelv kiberbiztonsággal kapcsolatos alapvető követelményeinek. A második szakaszban 2027. december 11-től alkalmazandóvá válik a kiberrezilienciáról szóló jogszabály.

[33]2019 decemberében az orvostechnikai eszközökkel foglalkozó együttműködési csoport az orvostechnikai eszközök kiberbiztonságáról szóló iránymutatást adott ki, hogy támogassa a gyártókat a két rendelet I. mellékletében foglalt követelmények teljesítésében: https://ec.europa.eu/docsroom/documents/41863.

[34]Az ENISA által 2020-ban kiadott, a kórházak kiberbiztonságára vonatkozó közbeszerzési iránymutatások alapján (2020. február). Elérhető a következő címen: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

továbbá a nemzeti és nemzetközi szabványoknak való megfelelésre irányuló ellenőrzések – szintén elengedhetetlenek a biztonsági gyakorlatok robusztusságának biztosításához.

Az olyan szolgáltatások tekintetében, mint az infrastruktúra-szolgáltatás (IaaS), a platformszolgáltatás (PaaS) és a szoftverszolgáltatás (SaaS), a biztonsági intézkedések végrehajtása gyakran az ügyfél feladata. Számos egészségügyi szervezet azonban nem rendelkezik elegendő forrással ahhoz, hogy az említett követelményeket önállóan teljesítse. Ezért **arra kell ösztönözni a felhőszolgáltatókat, hogy bizonyos biztonsági alapkövetelményeket alapértelmezett jelleggel építsenek be szolgáltatásaikba**. Ezek az intézkedések csökkentenék a hibás konfigurációk kockázatát, következetes védelmet biztosítanának az ügyfelek által kezelt környezetben, és nagyobb biztonságot nyújtanának a felhasználók számára. Az alapértelmezett biztonsági alapkövetelmények meghatározása során egyensúlyt kell teremteni a robusztus védelem és a gyakorlati alkalmazhatóság között, az egészségügyi szervezetek széles köre számára biztosítva a használhatóságot. Ez a lépés a felhőszolgáltatók és az egészségügyi ágazat szoros együttműködését kívánná, amelynek keretében a hatékony és igény szerint méretezhető megoldások kialakítása érdekében kihasználnák az iparág bevált gyakorlatait.

*Képzés és készségfejlesztés*

Európa hosszú távon fenntartható növekedése és versenyképessége, valamint a magas színvonalú szolgáltatások, köztük az egészségügyi szolgáltatások szempontjából is fontos, hogy a munkaerő rendelkezzen azokkal a készségekkel, amelyekre a legnagyobb szükség van. Európa-szerte komoly kihívást jelent a szakemberhiány: a becslések szerint 299 000 képzett kiberbiztonsági szakemberre van szükség az uniós munkaerő-szükséglet kielégítéséhez[35]. A kiberkészségekről szóló 2024. évi Eurobarométer felmérés[36] szerint a vállalatok 81 %-a szerint jelentős kockázat az esetleges kibertámadások tekintetében, hogy csak nehezen tudnak kiberbiztonsági személyzetet felvenni. Az oktatás, az egészségügy és a szociális munka ágazatában a kiberbiztonsági feladatkörök 66 %-át nem kiberbiztonsággal foglalkozó munkakörből érkező munkavállalók látják el, ami rávilágít arra, hogy sürgős szükség van átképzésre és továbbképzésre.

E kihívás kezeléséhez a Támogató Központnak együtt kell működnie a majdan létrehozandó, kiberbiztonsági készségekkel foglalkozó európai digitális infrastruktúra-konzorciummal (EDIC), amelyet a Kiberkészségek Akadémiájáról szóló bizottsági közlemény[37] irányoz elő. A munkájuknak elő kell segítenie az egészségügyi ágazat kiberbiztonsággal foglalkozó szakemberei, például az információbiztonsági főtisztivelők (CISO-k) közötti információcserét. Az egyik lehetséges intézkedés az **egészségügyi CISO-k európai hálózatának** létrehozása lenne; kezdetben egy szakértőkből álló csoportról lenne szó, akik megosztják és továbbfejlesztik a bevált gyakorlatokat, a tehetségmegtartási

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study (A kiberbiztonsági környezet 2024-ben: az ISC2 kiberbiztonságról szóló alkalmazotti tanulmányának eredményei) | Digitális Készségek és Munkahelyek Platformja.

[36] 547. sz. Eurobarométer gyorsfelmérés a kiberkészségekről.

[37] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A kiberbiztonsági szakemberhiány megszüntetése az EU versenyképességének, növekedésének és rezilienciájának növelése érdekében („Kiberkészségek Akadémiája”) COM(2023) 207 final.

stratégiákat és a kiberbiztonsággal foglalkozó szakemberek egészségügyi ágazatba való vonzására irányuló megoldásokat. Emellett a Kiberkészségek Akadémiájának égisze alatt erőforrásokat kell kifejleszteni a kiberbiztonsági munkaerő készségeinek javítására az egészségügyi ágazatban, az ipar és a tudományos körök támogatásával. Ennek keretében arra kell ösztönözni az ágazati érdekelt feleket, hogy kötelezzék el magukat a kiberbiztonsággal foglalkozó képzések támogatása mellett.

Az emberi hibák továbbra is jelentősen hozzájárulnak az egészségügyben bekövetkező kiberbiztonsági incidensekhez, ami rávilágít arra, hogy elengedhetetlen az egész személyzetre kiterjedő képzés és a kiberbiztonsági tudatosság. Az egészségügyi szakemberek gyakran használnak digitális eszközöket, ezért létfontosságú, hogy ismerjék a biztonságos gyakorlatokat. A célzott képzések és figyelemfelhívó kampányok nagyban csökkenthetik a kockázatokat. Ennek érdekében a Támogató Központnak együtt kell működnie az egészségügyi szakemberekkel és szolgáltatókkal, valamint az oktatási és képzési szolgáltatókkal, az ágazattal, a kiberbiztonsági készségekkel foglalkozó európai digitális infrastruktúra-konzorciummal, továbbá a tagállami hatóságokkal, hogy **kiterjedt és könnyen hozzáférhető online képzési modulokat és tanfolyamokat** hozzanak létre és terjesszenek.

A digitális kompetenciák és a kiberbiztonsági modulok tantervekbe való beépítése elengedhetetlen ahhoz, hogy az egészségügy kiberbiztonsága jól meg legyen alapozva. Az említett moduloknak foglalkozniuk kell az olyan ágazatspecifikus kérdésekkel, mint a betegadatok védelme és az orvostechnikai eszközök biztonságával kapcsolatos sérülékenység. Ezen ismeretanyagok kidolgozása során figyelembe kell venni az olyan korábbi intézkedéseket, mint az Erasmus+ program keretében finanszírozott BeWell projekt[38] és a Horizont 2020 keretében finanszírozott PANACEA projekt[39].

### *3.2.Európai képességek az egészségügyi ágazat elleni kiberfenyegetések felderítésére*

A kiberfenyegetések hatékony észlelése elengedhetetlen az incidensekre való gyors reagáláshoz. A fenyegető szereplők olyan technikákat tudnak alkalmazni, amelyek megnehezítik a behatolások észlelését, és ezáltal hosszabb ideig tudnak engedély nélkül hozzáférni egy adott rendszerhez[40]. A jobb fenyegetésészlelési képességek segíthetnek tehát a kibertámadások megállításában. Például a Vastaamo nevű finn pszichoterápiás szolgáltató elleni zsarolóvírusos támadás esetében – amelynek során az elkövetők megzsarolták azokat a betegeket, akiknek megszerezték a bizalmas egészségügyi dokumentációját – az első behatolás 2018-ban történt, de a szolgáltató csak 2020-ban szerzett róla tudomást[41].

[38]BeWell – Ágazati együttműködési terv a digitális és zöld készségekkel kapcsolatos jövőbeli egészségügyi munkaerő-stratégiához. Elérhető a következő címen: https://bewell-project.eu/.
[39]PANACEA – Adatvédelem és a magánélet védelme a kórházi és egészségügyi infrastruktúrákban, az intelligens kiberbiztonság, valamint a kiberfenyegetésekkel kapcsolatos, adatokat és embereket érintő eszköztárak révén. Elérhető a következő címen: https://cordis.europa.eu/project/id/826293.
[40]Az ENISA 2023. évi fenyegetettségi helyzetjelentése az egészségügyi ágazatról.
[41]A finn adatvédelmi ombudsman 1150/161/2021. sz. határozata.

A hatékony információmegosztás és együttműködés elengedhetetlen ahhoz, hogy Unió-szerte jobban észleljék a fenyegetéseket és javuljon a helyzetismeret. A számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) létfontosságú szereppel bírnak, mivel ők fogadják a biztonsági eseményekről, a majdnem bekövetkezett (near miss) eseményekről és a potenciális fenyegetésekről szóló bejelentéseket, valamint iránymutatást nyújtanak a nemzeti szintű kockázatcsökkentő intézkedésekkel kapcsolatban. **A Bizottság azonban határozottan arra ösztönzi a tagállamokat, hogy az uniós helyzetismeret kialakítása érdekében az ENISA Támogató Központjával is osszák meg a kórházaktól és az egészségügyi szolgáltatóktól származó valamennyi kiberbiztonsági incidensről szóló értesítést**. Ezt lehetőleg az incidensek különböző releváns dimenzióinak érdemi leírásával kell kiegészíteni, beleértve az incidenst kiváltó ismert sérülékenységeket, valamint az egészségügyi szolgáltatásokra és a betegeket érintő nemkívánatos eseményekre gyakorolt hatásokat is. Emellett a Bizottság az orvostechnikai és in vitro diagnosztikai eszközök gyártóit is arra ösztönzi, hogy a kiberrezilienciáról szóló jogszabály keretében az ENISA által létrehozandó és kezelendő egységes jelentéstételi platformon keresztül tegyenek önkéntes bejelentést azokkal az aktívan kihasznált sérülékenységekkel vagy súlyos kiberbiztonsági incidensekkel kapcsolatban, amelyek hatással vannak az említett eszközök biztonságára, valamint adott esetben jelentsék be az egyéb olyan sérülékenységeket, incidenseket, majdnem bekövetkezett (near miss) eseményeket vagy kiberfenyegetéseket, amelyek hatással lehetnek a szóban forgó eszközök kockázati profiljára.

Ha a bejelentésekben szereplő információk már nem minősülnek érzékenynek, a Támogató Központ összeállíthat egy, az ENISA által finanszírozott katalógust azokról az ismert kihasznált sérülékenységekről, amelyek az orvostechnikai eszközöket, az elektronikus egészségügyi nyilvántartó rendszereket, valamint az egészségügyi IKT-berendezések és -szoftverek szolgáltatóit érintik. A fenyegetések észlelésével kapcsolatos jelentős kihívások kezelése érdekében a Támogató Központnak olyan, **feliratkozáson alapuló és az egész Unióra kiterjedő korai előrejelző szolgáltatást kell bevezetnie az egészségügyi ágazat számára, amely közel valós idejű figyelmeztetéseket küld**. Ez a szolgáltatás olyan, már feldolgozott adatokra támaszkodna, amelyek a CSIRT-ektől, az egészségügyi szervezetektől és gyártóktól, a nyílt forrásból származó értékelt felderítésekből (OSINT) és más érintett szereplőktől, például a kiberközpontoktól, az információmegosztó és -elemző központoktól (ISAC) és a bűnüldöző hatóságoktól származnak. Az ENISA és a Bűnüldözési Együttműködés Európai Uniós Ügynöksége (Europol) közötti megerősített együttműködés – például az egészségügyi ágazat elleni kiberbűnözés mintáit érintően – tovább fokozná a helyzetismeretet.

Az információmegosztó és -elemző központok központi forrásként szolgálnak a fenyegetettséggel kapcsolatos hírszerzéshez, azáltal, hogy elősegítik a kétirányú információmegosztást a köz- és a magánszektor között, valamint előmozdítják a bizalomépítést. A Támogató Központnak fokoznia kell az **európai egészségügyi információmegosztó és -elemző központ (ISAC)** támogatását, mégpedig eszközökkel és információcserével, ágazati helyzetismereti jelentések kiadásával, valamint a taktikai és stratégiai együttműködés célját szolgáló megbízható közösség létrehozásával. A tagállamoknak ösztönözniük kell az egészségüggyel foglalkozó nemzeti információmegosztó és -elemző központok

kialakítását[42]. Az információmegosztó és -elemző központokat is arra kell ösztönözni, hogy hozzák össze az egészségügyi szolgáltatókat és a gyártókat, hogy azok – többek között az ellátási lánc tekintetében – közös álláspontot alakítsanak ki a kiberfenyegetésekkel kapcsolatban, és egy olyan párbeszéd alakuljon ki a termékek biztonságos tervezéséről, amely valóban figyelembe veszi a konkrét megvalósítási lehetőségeket.

### *3.3. Gyors reagálás és helyreállítás*

Tekintettel a betegek egészségügyi adatainak nagy fokú érzékenységére és arra, hogy a kibertámadások milyen pusztító hatással lehetnek az egészségügyi szolgáltatásokra, a kiberbiztonsági incidensekre való gyors és hatékony reagálás elengedhetetlen a betegbiztonság védelméhez. Ha egy kórház vagy egy egészségügyi szolgáltató kibertámadással szembesül, az elsődleges kapcsolattartó pont a releváns nemzeti CSIRT[43]. A CSIRT feladata, hogy kellő időben, ideális esetben 24 órán belül támogatást nyújtson a jelentős incidensek kezeléséhez. Ha azonban egy incidens meghaladja a CSIRT kapacitását, rendelkezésre kell állnia a gyors és hatékony reagálást biztosító uniós támogatásnak.

A kiberszolidaritásról szóló jogszabály alapján létrehozott uniós kiberbiztonsági tartalék megbízható irányított biztonsági szolgáltatók által nyújtott, incidensekre reagáló szolgáltatásokat tesz elérhetővé, hogy segítséget nyújtson a jelentős vagy nagyszabású kiberbiztonsági incidensek esetén, és támogassa a kezdeti helyreállítási erőfeszítéseket. E tartalék célja, hogy kiegészítse a tagállami CSIRT-ek erőfeszítéseit, lehetővé téve számukra, hogy további támogatást kérhessenek az olyan kritikus ágazatokat érintő esetekben, mint az egészségügy. E rendszer továbbfejlesztése érdekében **a Bizottságnak és az ENISA-nak biztosítania kell, hogy a tartalék részét képezze egy kifejezetten az egészségügyi ágazatra vonatkozó gyorsreagálási szolgáltatás** is. Ez a szolgáltatás kiegészítene más, már meglévő kereteket, és gondoskodna a szakértők haladéktalan bevetéséről az egészségügyben bekövetkező jelentős vagy nagyszabású kiberbiztonsági incidensek kezelésének érdekében, amennyiben a nemzeti támogatás nem bizonyul elegendőnek.

A hatékonyabb reagálás és helyreállítás érdekében a Támogató Központnak a Kiberbiztonsági Együttműködési Csoporttal, a CSIRT-ek hálózatával és adott esetben az Europollal együttműködésben kifejezetten az egészségügyi ágazat részére ki kell dolgoznia**a kiberbiztonsági incidensekkel kapcsolatos válaszprotokollokat**. Ezek a válaszprotokollok iránymutatással szolgálnának mind a CSIRT-ek, mind az egészségügyi szervezetek számára a konkrét kiberfenyegetésekre, többek között a zsarolóvírusokra való reagálás tekintetében. Tekintettel a CSIRT-ek és a bűnüldöző hatóságok közötti hatékony együttműködés fontosságára a büntetőjogi jellegű kiberbiztonsági incidensekre való reagálás

[42]Finnországban például már létezik a szociális jóléttel és az egészségügyi ágazattal foglalkozó nemzeti információmegosztó és -elemző központ. Lásd: Finn Nemzeti Kiberbiztonsági Központ: „ISAC information sharing groups” (ISAC információmegosztó és -elemző központok), elérhető a következő címen: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43]A NIS 2 irányelv 23. cikkének (1) bekezdése előírja, hogy az alapvető és fontos szervezeteknek értesíteniük kell a releváns CSIRT-t vagy adott esetben az illetékes hatóságot minden jelentős incidensről.

és azok kivizsgálása terén, a válaszprotokolloknak többek között egyértelmű iránymutatást kell nyújtaniuk az ilyen események bűnüldöző szervek felé történő bejelentéséhez. Emellett a Támogató Központ – **az ENISA 2022. évi Cyber Europe gyakorlatához hasonló gyakorlatok tapasztalataira építve – segítséget nyújthat a nemzeti kiberbiztonsági gyakorlatok széles körű lebonyolításához, az incidensekre való reagálás válaszprotokolljainak tesztelése és megerősítése érdekében**.

A szakpolitikák megalapozása és a zsarolóvírus-támadások elleni intézkedések hatékonyságának értékelése érdekében további adatokat kell gyűjteni. E célból a tagállamoknak fel kell kérniük a NIS 2 irányelv hatálya alá tartozó szervezeteket, köztük az egészségügyi szervezeteket, hogy a jelentős kiberbiztonsági incidensekről való jelentéstétel során szolgáltatott egyéb információk mellett jelentsék be a már teljesített és a teljesíteni kívánt váltságdíjfizetéseket is. Az említett jelentéstétel támogatja a zsarolóvírussal kapcsolatos incidensek hatékony kivizsgálását, beleértve a kifizetések nyomon követését a kriptovaluta-csereplatformokon, a címzettek azonosítása érdekében.

A helyreállítás sebessége kritikus tényező a reziliencia és a közvélemény bizalmának fenntartásának szempontjából, különösen az egészségügyben, ahol a leállás zavart okozhat a betegellátásban. A zsarolóvírus-támadásokat követő hatékony helyreállítás érdekében az egészségügyi szolgáltatóknak biztonságos, naprakész és elkülönített biztonsági másolatokkal kell rendelkezniük, amelyek gyorsan helyreállíthatók. Szolgáltatáskatalógusának részeként a Támogató Központ kínálhat **a működés zsarolóvírusos támadások utáni helyreállítását segítő, feliratkozáson alapuló szolgáltatást, amely támogatja a kórházakat és az egészségügyi szolgáltatókat a helyreállítási tervek előzetes elkészítésében.** Az ENISA-nak és az Europolnak együtt kell működnie az egészségügyi szervezeteket célzó leggyakoribb zsarolóvírustörzsek azonosítása érdekében, és ki kell bővítenie a „No More Ransom" projekt[44] keretében rendelkezésre álló **dekódoló eszközök adattárát**. Emellett hozzáférhető iránymutatásokat kell kidolgozniuk és terjeszteniük, hogy segítségükkel az egészségügyi szolgáltatók a dekódoló eszközök használatának köszönhetően elkerülhessék a váltságdíjfizetést.

A **zsarolóvírusok elleni nemzetközi kezdeményezés**[45] értékes fórum a konkrét zsarolóvírus-incidensekkel kapcsolatos információcseréhez, valamint a tagállamok azon kapacitásainak kiépítéséhez, hogy megerősítsék a kiberbiztonsággal kapcsolatos kereteiket és javítsák a zsarolóvírussal fenyegető szereplőkkel szembeni vizsgálati képességeiket. A Bizottság a főképviselővel együttműködésben továbbra is elő fogja mozdítani a zsarolóvírusok elleni kezdeményezés keretében folytatott együttműködést, többek között az egészségügyi ágazatot célzó zsarolóvírus-fenyegetések ellen. Emellett a Bizottság együttműködésre fog törekedni a **G7-ek kiberbiztonsággal foglalkozó bizottságközi munkacsoportján belül** az egészségügyi ágazat kiberbiztonságának megerősítése érdekében. A munkacsoport mérlegelheti, hogy miként lehet támogatni az egészségügyi ágazatot az olyan fenyegetésekkel szemben, mint például a zsarolóvírusok, többek között az Egyesült Nemzetek Biztonsági Tanácsának keretében előterjesztett, az egészségügyi létesítmények elleni zsarolóvírus-támadásokról szóló, 2024. november 8-i közös nyilatkozatra[46] építve.

[44] https://www.nomoreransom.org/en/index.html.
[45] https://www.counter-ransomware.org/.
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.

## 4. Nemzeti intézkedések

Az, hogy e cselekvési terv mennyire képes javítani az egészségügyi ágazat kiberbiztonságát, a tagállamok aktív részvételétől és elkötelezettségétől függ. A cselekvési terv sikeres végrehajtása érdekében a tagállamok kijelölhetnek olyan **nemzeti kiberbiztonsági támogató központokat, amelyek kifejezetten a kórházakkal és az egészségügyi szolgáltatókkal foglalkoznak**. Ezek a központok lennének az elsődleges kapcsolattartó pontok az egészségügyi ágazat számára nemzeti szinten, és szorosan együttműködnének az ENISA Támogató Központjával. Amennyiben lehetséges és releváns, a tagállamoknak meglévő szerveket, például a nemzeti egészségügyi CSIRT-eket vagy az illetékes hatóságokat kell nemzeti kiberbiztonsági támogató központként kijelölniük.

A Bizottság arra is ösztönzi a tagállamokat, hogy dolgozzanak ki az **egészségügyi ágazat kiberbiztonságára összpontosító nemzeti cselekvési terveket**. Ezek a tervek felvázolnák az egészségügyi rendszereket érintő konkrét kiberbiztonsági kockázatokat és a kezelésükre irányuló nemzeti intézkedéseket, miközben biztosítanák az európai szintű erőforrások és gyakorlatok hatékony felhasználását is. Az ENISA Támogató Központja segítséget nyújthat e tervek kidolgozásában, figyelembe véve a már meglévő nemzeti terveket, és elősegítve az erőfeszítések összehangolását, hogy az egyes tagállamok erőforrásai és stratégiái kiegészítsék egymást.

A tagállamok másik kulcsfontosságú feladata annak elősegítése, hogy az egészségügyi szolgáltatók osztozzanak az erőforrásokon, ami nemzeti, regionális vagy akár európai szintű **közös beszerzésekkel vagy az erőforrások egyesítésével** érhető el. Ez a megközelítés csökkentené az egyes szervezetekre nehezedő pénzügyi terheket, miközben megerősítené a tárgyalási pozíciójukat a kiberbiztonsági szolgáltatókkal szemben.

A francia CaRE program[47] például számos nemzeti és regionális szintű intézkedést vezetett be az erőforrásokkal kapcsolatos kihívások kezelésére: egy kiberkatalógus a kereskedelmi forgalomban elérhető megoldások mellett áttekintést ad azokról a kiberbiztonsággal kapcsolatos megoldásokról és csomagokról is, amelyeket a nemzeti kiberbiztonsági ügynökség, a digitális egészségügyi ügynökség, a regionális ügynökségek és a nemzeti beszerzési szervezetek bocsátanak a kórházak rendelkezésére. Emellett a regionális ügynökségek további finanszírozásban részesülnek, hogy megosztott forrásokat kínálhassanak.

A tagállamoknak foglalkozniuk kell azzal is, hogy az egészségügyi ágazaton belül nem történik elég beruházás a kiberbiztonság területén. A megfelelő finanszírozás biztosítása érdekében **nem kötelező erejű referenciaértékeket kell meghatározniuk, és nyomon kell követniük a kifejezetten a**

[47]Francia Digitális Egészségügyi Ügynökség: Cybersécurité acceleration et Résilience des Établissements (CaRE). Elérhető a következő címen: https://esante.gouv.fr/strategie-nationale/cybersecurite.

**kiberbiztonságra irányuló finanszírozási célértékeket**, ugyanakkor biztosítaniuk kell, hogy ezek a beruházások ne váljanak az alapvető betegellátás kárára. Ezeknek a finanszírozási célértékeknek egyben arra is kell irányulniuk, hogy a biztonsági megfontolások integrálva legyenek az ágazat valamennyi digitális beruházásába. A tagállamok az olyan platformokon keresztül, mint az e-egészségügyi hálózat[48] megoszthatják egymással az e célértékekkel kapcsolatban bevált gyakorlatokat, és tanácsokkal láthatják el egymást.

## 5. A közszféra és a magánszféra közötti együttműködés

A cselekvési terv sikeres végrehajtásához elengedhetetlen a köz- és a magánszféra közötti együttműködés, valamint az egészségügyi szolgáltatókkal, az egészségügyi ágazat egyéb szervezeteivel és a kiberbiztonsági ágazat érintett szereplőivel folytatott konzultáció. A Támogató Központ munkájához való további hozzájárulás érdekében **a Bizottság az ENISA támogatásával közös egészségügyi kiberbiztonsági tanácsadó testületet hoz létre**, amely mindkét terület – az egészségügy és a kiberbiztonság – magas szintű képviselőiből áll, és tanácsot adhat a Bizottságnak és a Támogató Központnak a leghatásosabb intézkedésekkel kapcsolatban, valamint megvitathatja a szóban forgó terület tekintetében a köz- és magánszféra közötti partnerségek továbbfejlesztését. A testület munkája a köz- és magánszféra közötti partnerségekre irányuló meglévő erőfeszítésekre, például az európai egészségügyi információmegosztó és -elemző központra (ISAC) fog támaszkodni.

A Bizottság továbbá **cselekvési felhívást** intéz a kiberbiztonsági vállalatokhoz, alapítványokhoz, oktatási intézményekhez és ágazat érdekelt feleihez, hogy **vállaljanak kötelezettséget az ágazat kihívásainak kezelése iránt**. A Kiberkészségek Akadémiájának tapasztalatai alapján ilyen kötelezettségvállalás lehet például egy olyan, a Kiberkészségek Akadémiája keretében tett vállalás, amely kiberbiztonsági szakembereknek szánt tanfolyamok és tananyagok biztosítására irányul, az egészségügyi ágazatra összpontosítva[49]. A kötelezettségvállalások irányulhatnak figyelemfelkeltő tevékenységekre is, vagy olyan, a kifejezetten kiszolgáltatott helyzetben lévő szervezetek számára ingyenesen vagy csökkentett költségtérítés ellenében nyújtott irányított biztonsági szolgáltatásokra, amelyek célja a felkészültség és a kiberbiztonsági reziliencia növelése. Ezen túlmenően a kötelezettségvállalások kiterjedhetnek a kiberfenyegetésekkel kapcsolatos hírszerzési információknak az ENISA Támogató Központjával történő megosztására. A cselekvési felhívás keretében tett vállalások áttekintése a Támogató Központ feladata lenne, amely biztosítaná azok koherenciáját és egymást kiegészítő jellegét.

## 6. A kibertámadással fenyegető szereplők elrettentése

Az EU belső és külső kiberbiztonsági politikáinak támogatniuk kell azt a célt, hogy a kibertámadással fenyegető szereplőket visszatartsák az európai egészségügyi rendszerek elleni támadásoktól. Az egészségügyi szervezetek elleni kibertámadások a rosszindulatú kibertevékenységek különösen elfogadhatatlan típusának számítanak, mivel veszélyt jelenthetnek a betegek biztonságára és az emberi

[48] Az e-egészségügyi hálózat a 2011/24/EU irányelv 14. cikke értelmében létrehozott önkéntes hálózat, amely a tagállamok által kijelölt, az e-egészségügyért felelős nemzeti hatóságokból állt.

[49] A Kiberkészségek Akadémiája:Vegyen Ön is részt! Digitális Készségek és Munkahelyek Platformja.

életekre nézve. Ezért a kiberbiztonság és a bűnüldözés területén teljes mértékben ki kell használni az EU elrettentési képességeit, hogy ellehetetlenüljön az egészségügyi ágazatot kibertámadással fenyegető szereplők általános üzleti modellje, és megszűnjön a könnyű nyereségszerzés lehetősége. Ennek keretében fokozni kell a határokon átnyúló nyomozásokat a fertőzöttségi mutatók és más releváns adatok megosztásának kiterjesztése révén, valamint nagyobb figyelmet kell irányítani a nagy értékű célpontokra és a legfőbb bűnsegélyezőkre, például a tartalomfelügyelet nélküli tárhelyszolgáltatókra vagy a kriptovaluta-mixerekre.

A **kiberdiplomáciai eszköztár** keretet biztosít az EU, a tagállamok és a partnerek elleni kibertámadások megelőzéséhez, megakadályozásához és az azokra való reagáláshoz. A főképviselő továbbra is alkalmazni fogja a meglévő kiberbiztonsági szankciós keretet az egészségügyi rendszereket érintő fenyegetésekre való reagálás során.

A bűnözők felelősségre vonása jelentős visszatartó erővel bír. Ezért a tagállamoknak biztosítaniuk kell, hogy a bűnüldözés teljes mértékben be legyen építve a nemzeti cselekvési tervükbe. Teljes mértékben ki kell használniuk az információs rendszerek elleni támadásokról szóló irányelvben[50] és az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményében előírt rendelkezéseket a támadásoktól való elrettentés, a bűnözők bíróság elé állítása és a támadásokat elősegítő bűnözői infrastruktúrák felszámolása érdekében[51]. Az említett eszközök sikeres alkalmazásával biztosítható, hogy az egészségügyi ellátás elleni bűncselekmények és rosszindulatú cselekmények büntetésben részesüljenek.

## 7. A cselekvési terv végrehajtása és nyomon követése

E cselekvési terv számos feladatot irányoz elő az ENISA-n belül létrehozandó Támogató Központ számára. Mindez biztosítja a cselekvési terv átfogó és következetes végrehajtását, elkerülve ugyanakkor az esetleges átfedésekhez és általános költségekhez vezető új szervezetek létrehozását. A Bizottság biztosítani kívánja a Támogató Központ számára a megfelelő erőforrásokat.

Amint a Támogató Központ megkezdi működését, az ENISA-nak a Bizottsággal konzultálva rendszeres tájékoztatást kell nyújtania a Támogató Központ tevékenységéről az ENISA igazgatótanácsának, valamint az érintett tagállami hálózatoknak, különösen a Kiberbiztonsági Együttműködési Csoportnak, a CSIRT-hálózatnak, az e-egészségügyi hálózatnak és adott esetben az Európai Egészségügyi Adattér Testületnek Az ENISA-nak továbbá folyamatos megbeszéléseket kell folytatnia a köz- és magánszférát összekötő egészségügyi kiberbiztonsági tanácsadó testülettel a Támogató Központ által biztosított intézkedések végrehajtásáról.

Az ENISA rendszeres jelentéseivel egyidejűleg – például az Unió kiberbiztonságának helyzetéről szóló jelentés közzétételekor, amely összesített értékelést nyújt a kiberbiztonsági képességeknek és erőforrásoknak az egész EU-ban, és ezen belül az egészségügyi ágazatban tapasztalható érettségi szintjéről – célszerű lenne nyilvánosságra hozni a releváns adatokat, ezáltal támogatva a cselekvési terv

[50]Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról: https://eur-lex.europa.eu/eli/dir/2013/40/oj/hun.
[51]A számítástechnikai bűnözésről szóló egyezmény (Budapesti Egyezmény, ETS 185. sz.) és jegyzőkönyvei: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

nyomon követését. Emellett az ENISA uniós kiberbiztonsági indexe[52] mennyiségi és minőségi adatokat szolgáltathat, amelyek tényanyagként szolgálhatnak az egészségügyi ágazat kritikusságának és érettségi szintjének értékelése során.

## 8. Következő lépések

Ez a közlemény ambiciózus menetrendet ír elő az uniós egészségügyi ágazat kiberbiztonságának fokozására. A Kórházak és Egészségügyi Szolgáltatók Kiberbiztonsági Támogató Központjának az ENISA szervezetén belül történő létrehozásával a cselekvési terv kijelöli az ágazat kiberbiztonsági kihívásaival kapcsolatos koherens és közös európai megközelítés kialakításának útját.

Ez a közlemény az egészségügyi ágazat kiberbiztonsági helyzetének javítására irányuló folyamatnak csupán a kezdete. A cselekvési terv elfogadását az érdekelt felekkel folytatott átfogó konzultációk indítása fogja kísérni, valamint folytatódnak a tagállamokkal és az érintett hálózatokkal az ismeretek összegyűjtése érdekében megkezdett megbeszélések. A konzultációk eredményei alapján a Bizottság 2025 negyedik negyedévében a cselekvési terv további finomítására vonatkozó ajánlásokat kíván előterjeszteni.

A Bizottság felkéri a tagállamokat és valamennyi érdekelt felet, hogy közösen dolgozzanak a cselekvési terv célkitűzéseinek megvalósításán.

[52]ENISA, Uniós kiberbiztonsági index, keret és módszertani feljegyzés (2024). Elérhető a következő címen: https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

**MELLÉKLET – A javasolt intézkedések áttekintése**

**Bizottság:**

| **A Kórházak és Egészségügyi Szolgáltatók Kiberbiztonsági Támogató Központja az ENISA-n belül** | |
|---|---|
| Megfelelő források biztosítása a Kiberbiztonsági Támogató Központ számára<br><br>Együttműködés az Európai Kiberbiztonsági Kompetenciaközponttal a legjobb kiberhigiéniai és -biztonsági kockázatértékelési gyakorlatok kidolgozására irányuló kísérleti projektek elindítása, valamint a kiberbiztonság folyamatos nyomon követése, a fenyegetettséggel kapcsolatos hírszerzés és az incidensekre való reagálás iránti igény kezelése érdekében, a legkorszerűbb kiberbiztonsági megoldások alkalmazásával, az Európai Kiberbiztonsági Támogató Központ szolgáltatáskatalógusának kidolgozása érdekében | 2025 |
| **A kiberbiztonsági incidensek megelőzése** | |
| A Kiberbiztonsági Együttműködési Csoporttal, az EU-CyCLONe-nal és az ENISA-val való konzultáció alapján annak feltérképezése, hogy az egészségügy azon ágazatok közé sorolható-e, amelyek a kiberszolidaritásról szóló jogszabály keretében támogatást kaphatnak összehangolt felkészültségi tesztelésre | 2025 első negyedéve |
| **Gyors reagálás és helyreállítás** | |
| Gyorsreagálási szolgáltatás biztosítása kifejezetten az egészségügyi ágazat számára, az uniós kiberbiztonsági tartalék keretében és az ENISA-val együttműködésben | 2025 negyedik negyedéve |
| **A közszféra és a magánszféra közötti együttműködés** | |
| Közös egészségügyi kiberbiztonsági tanácsadó testület létrehozása az ENISA támogatásával | 2025 első negyedéve |
| Cselekvési felhívás közzététele a kiberbiztonsági vállalatok, alapítványok, oktatási intézmények és az ágazat érdekelt felei számára, hogy vállaljanak kötelezettséget az egészségügyi ágazat kihívásainak kezelése iránt | 2025 második negyedéve |
| **A kibertámadással fenyegető szereplők elrettentése** | |

| | |
|---|---|
| A kiberdiplomáciai eszköztár használatának a főképviselővel együttműködésben történő feltérképezése az egészségügyi rendszerek elleni rosszindulatú tevékenységek megelőzése, az ilyen tevékenységektől való elrettentés és az azokra való reagálás érdekében | 2025 |
| A zsarolóvírussal fenyegető szereplőkkel szembeni nemzetközi együttműködés előmozdítása, különösen a zsarolóvírusok elleni nemzetközi kezdeményezés keretében, együttműködésben a főképviselővel | 2025–2026 |
| Törekvés a G7-ek kiberbiztonsággal foglalkozó bizottságközi munkacsoportján belül az egészségügyi ágazat kiberbiztonságának megerősítése érdekében történő együttműködésre | 2025–2026 |
| **Következő lépések** | |
| Az érdekelt felekkel folytatott átfogó konzultációk indítása | 2025 első negyedéve |
| Ajánlások előterjesztése a cselekvési terv további finomhangolása érdekében | 2025 negyedik negyedéve |

**ENISA:**

| **Kórházak és Egészségügyi Szolgáltatók Európai Kiberbiztonsági Támogató Központja** | |
|---|---|
| A Kórházak és Egészségügyi Szolgáltatók Európai Kiberbiztonsági Támogató Központjának létrehozására irányuló munka megkezdése | 2025 második negyedéve |
| A Kiberbiztonsági Támogató Központ által biztosítandó átfogó szolgáltatáskatalógus kidolgozása | 2025 negyedik negyedévétől kezdve |
| **A kiberbiztonsági incidensek megelőzése** | |
| Iránymutatás kiadása, amely kiemeli a legfontosabb kiberbiztonsági gyakorlatokat, és segítséget nyújt az egészségügyi szolgáltatóknak azok végrehajtásában | 2025 harmadik negyedéve |
| A szabályozás feltérképezésére eszköz kidolgozása, szoros együttműködésben a Bizottsággal és a tagállamokkal | 2025 első negyedéve |

| | |
|---|---|
| A kiberbiztonsági érettségi szint kifejezetten az egészségügyre vonatkozó értékelési keretének kidolgozása | 2025 harmadik negyedéve |
| Éves egészségügyi kiberérettségi értékelés elvégzése | 2025–2026 |
| Együttműködés a tagállamokkal és a regionális programhatóságokkal a kiberbiztonsági utalványok mintaprogramjainak létrehozásáért | 2025–2026 |
| A kórházak és az egészségügyi szolgáltatók kiberbiztonságára vonatkozó új közbeszerzési iránymutatások kidolgozása | 2025 harmadik negyedéve |
| Az egészségügyi CISO-k európai hálózatának létrehozása | 2026 első negyedéve |
| Egészségügyi szakemberek számára biztosított kiberbiztonsági modulok és tanfolyamok megtervezése és népszerűsítése | 2026 első negyedéve |
| **Európai képességek az egészségügyi ágazat elleni kiberfenyegetések felderítésére** | |
| Az orvostechnikai eszközöket, az elektronikus egészségügyi nyilvántartó rendszereket, valamint az egészségügyi IKT-berendezések és -szoftverek szolgáltatóit érintő ismert kihasznált sérülékenységek katalógusának összeállítása | 2025 negyedik negyedéve |
| A feliratkozáson alapuló és az egész Unióra kiterjedő korai előrejelző szolgáltatás bevezetése az egészségügyi ágazatban | 2026-tól |
| Az európai egészségügyi információmegosztó és -elemző központ (ISAC) eszközök és információcsere révén történő támogatása | 2025–2026 |
| **Gyors reagálás és helyreállítás** | |
| Gyorsreagálási szolgáltatás biztosítása kifejezetten az egészségügyi ágazat számára, az uniós kiberbiztonsági tartalék keretében és a Bizottsággal együttműködésben | 2025 negyedik negyedéve |
| Az egészségügyre szabott, a kiberbiztonsági incidensekkel kapcsolatos válaszprotokollokról szóló ismertetők kidolgozása a CSIRT-hálózattal együttműködésben | 2025 harmadik negyedéve |

| | |
|---|---|
| Nemzeti kiberbiztonsági gyakorlatok széles körű lebonyolításának elősegítése az incidensekre való reagálás válaszprotokolljainak tesztelése és megerősítése érdekében | 2025 negyedik negyedévétől |
| A működés zsarolóvírusos támadások utáni helyreállítását segítő, feliratkozáson alapuló szolgáltatás nyújtása | 2026-tól |
| Együttműködés az Europollal az egészségügyi szervezeteket célzó leggyakoribb zsarolóvírustörzsek azonosítása érdekében, valamint a dekódoló eszközök adattárának bővítése a „No More Ransom” projekt keretében | 2025 negyedik negyedéve |
| Hozzáférhető iránymutatások kidolgozása az Europollal együttműködésben annak érdekében, hogy az egészségügyi szolgáltatók elkerülhessék a váltságdíjfizetést | 2025 harmadik negyedéve |
| **Nemzeti intézkedések** | |
| Segítségnyújtás a tagállamoknak a nemzeti cselekvési tervek kidolgozásában | 2025 |
| Az erőfeszítések összehangolása annak érdekében, hogy az egyes tagállamok erőforrásai és stratégiái kiegészítsék egymást | 2025–2026 |
| **A cselekvési terv végrehajtása és nyomon követése** | |
| Rendszeres tájékoztatásnyújtás a Kiberbiztonsági Támogató Központ tevékenységéről az érintett tagállami hálózatoknak, a Bizottsággal konzultálva | 2025–2026 |
| Folyamatos eszmecsere az egészségügyi kiberbiztonsági tanácsadó testülettel | 2025–2026 |

**Tagállamok:**

| | |
|---|---|
| **Európai képességek az egészségügyi ágazat elleni kiberfenyegetések felderítésére** | |
| A kórházaktól és az egészségügyi szolgáltatóktól kapott incidensbejelentések megosztása az európai Kiberbiztonsági Támogató Központtal a NIS 2 irányelv keretében | 2025 negyedik negyedévétől |

| | |
|---|---|
| Az egészségüggyel foglalkozó nemzeti információmegosztó és -elemző központok kialakításának ösztönzése. | 2025–2026 |
| **A kiberbiztonsági incidensek megelőzése** | |
| Összehangolt biztonsági kockázatértékelés elvégzése a Kiberbiztonsági Együttműködési Csoporton belül az orvostechnikai eszközök ellátási láncaival kapcsolatos technikai és stratégiai kockázatok felmérésére | 2025 negyedik negyedéve |
| **Gyors reagálás és helyreállítás** | |
| Nemzeti kiberbiztonsági gyakorlatok széles körű lebonyolítása, az incidensekre való reagálás válaszprotokolljainak tesztelése és megerősítése érdekében | 2026-tól |
| **Nemzeti intézkedések** | |
| Nemzeti kiberbiztonsági támogató központok kijelölése a kórházak és egészségügyi szolgáltatók számára | 2025 második negyedéve |
| Az egészségügyi ágazat kiberbiztonságára összpontosító nemzeti cselekvési tervek kidolgozása | 2025 negyedik negyedéve |
| Az egészségügyi szolgáltatók közötti erőforrás-megosztás elősegítése | 2025–2026 |
| Nem kötelező erejű referenciaértékek meghatározása és a kifejezetten a kiberbiztonságra irányuló finanszírozási célértékek nyomon követése | 2025 negyedik negyedéve |
| Az egészségügyi szervezetek és a NIS 2 irányelv hatálya alá tartozó egyéb szervezetek felszólítása arra, hogy jelentsék be váltságdíjfizetésre irányuló szándékukat | 2025 negyedik negyedéve |