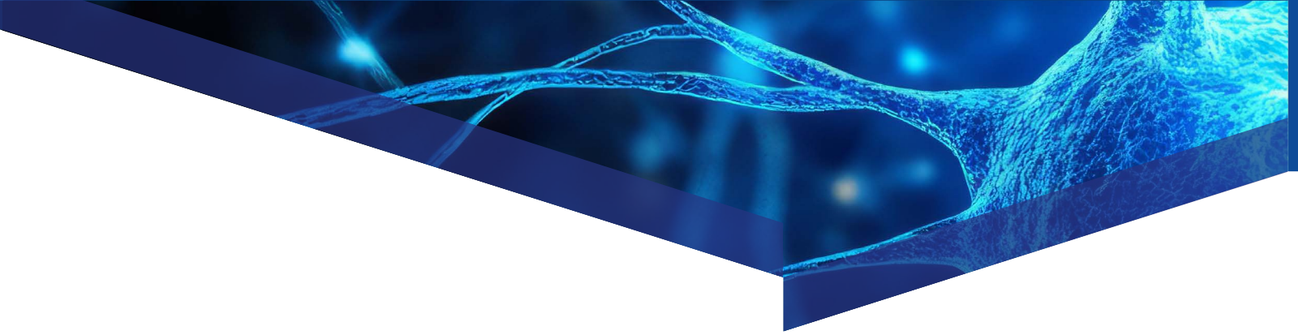
CTI jelentés

BCI rendszerek kiberbiztonsága

1996
Fortes fortuna adiuvat
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERVÉDELMI INTÉZET



Tartalomjegyzék

Bevezetés

Az agy-számítógép interfész (Brain-Computer Interface - BCI) rendszerek és az agyba ültethető orvostechnikai eszközök megjelenése új korszakot nyitott a neurológiai betegségek kezelésében és a fogyatékossággal élők életminőségének javításában. Ezek a technológiák alapvetően abban különböznek a hagyományos orvostechnikai eszközöktől, hogy közvetlen összeköttetést teremtenek az idegrendszer és a digitális informatikai rendszerek között, ezáltal lehetővé teszik a gondolatvezérelt protézisek, adaptív stimulációs programok és szenzoros visszacsatolások működését.

Az elmúlt években a fejlesztések középpontjába került a valós idejű neurális adatelemzés, amely egyre inkább épít mesterséges intelligencia algoritmusokra és felhőalapú számítási környezetekre. Míg a korábbi generációs implantátumok zárt protokollokkal és offline működéssel jellemezhetők, az új eszközök már hálózati kapcsolattal rendelkeznek, rendszeresen frissíthetők, és távoli felügyeletet biztosítanak. Ez a paradigmaváltás nagyságrendekkel növeli a kiberbiztonsági kockázatokat, hiszen a támadási felület kiterjed a beültetett firmware-ekre, a kommunikációs csatornákra, a mobilalkalmazásokra és a felhőalapú adatbázisokra egyaránt.

A neurális jelek különleges érzékenysége miatt a BCI rendszerek kompromittálása nemcsak adatvédelmi incidenseket eredményezhet, hanem súlyos neurológiai és pszichológiai következményeket is. Egy rosszindulatú támadó potenciálisan képes lehet a szenzoradatok manipulálására, a stimulációs protokollok módosítására vagy a készülék működésének blokkolására. A következmények között szerepelhet a beteg döntéshozatali képességének befolyásolása, idegrendszeri károsodás vagy akár életveszélyes állapot kialakulása. Ez a helyzet minden más orvostechnikai eszközhöz képest példátlan felelősségi és etikai dilemmát teremt.

A technológiai fejlődés tempóját a nemzetközi és hazai kutatási programok is ösztönzik, amelyek egyre szélesebb körben alkalmazzák a BCI rendszereket terápiás és rehabilitációs célokra. Ugyanakkor a jogi szabályozás, az etikai irányelvek és a kiberbiztonsági követelmények gyakran nem képesek lépést tartani az innováció sebességével. A Medical Device Regulation (MDR), a GDPR és az egyes országok belső szabályozása számos kötelezettséget rögzít, de a neurális adatok, a távoli firmware-frissítés és az AI-alapú döntéstámogatás kérdései sok tekintetben továbbra is rendezetlenek.

A tanulmány célja, hogy átfogó képet nyújtson a BCI rendszerek és agyi implantátumok kiberbiztonsági, jogi és etikai környezetéről, különös tekintettel a valós sebezhetőségekre, a támadási technikákra és a gyakorlati tapasztalatokra. Az elemzés bemutatja a releváns szabályozási kereteket, a technológiai architektúrákat és a kockázatcsökkentési lehetőségeket, miközben esettanulmányokkal illusztrálja, hogy a kihívások már nem elméleti természetűek, hanem a mindennapi klinikai gyakorlat részévé váltak.

Szabályozási környezet és megfelelőségi követelmények

Az agyba ültethető orvostechnikai eszközök és a BCI rendszerek jogi szabályozása világszerte gyorsan fejlődő, mégis széttagolt keretrendszerben történik, amelyben az adatvédelem, a betegbiztonság és a technológiai megfelelőség elvei gyakran egymással versengő prioritásokat képviselnek. Az Európai Unióban a legfontosabb jogszabályi alapot az (EU) 2017/745 rendelet adja, amelyet Medical Device Regulation (MDR) néven ismerünk. Ez a rendelet a BCI rendszerek nagy részét a III. kockázati osztályba sorolja, amely a legszigorúbb minősítési követelményeket és klinikai bizonyítási kötelezettséget írja elő. Az MDR egyértelműen rögzíti, hogy minden orvostechnikai eszköznél kötelező a kiberbiztonsági kockázatok teljes körű elemzése és dokumentálása a teljes életciklus alatt, beleértve a tervezést, a gyártást, az üzemeltetést és a leszerelést is.

A szabályozás szerint a gyártóknak gondoskodniuk kell arról, hogy a készülékek adatintegritása és hitelessége minden kommunikációs és adattovábbítási folyamat során garantált legyen. A kockázatkezelési dokumentációban rögzíteni kell a frissítési protokollokat, a szoftververziók visszakövethetőségét és a jogosulatlan hozzáférés megakadályozására tett intézkedéseket.

Az MDR mellett 2023-ban életbe lépett a NIS2 irányelv, amely az alapvető szolgáltatást nyújtó szervezetekre, köztük az egészségügyi intézményekre is kiterjeszti a szigorú kiberbiztonsági kötelezettségeket. A NIS2 szabályai értelmében egy biztonsági incidens észlelése után legfeljebb 72 órán belül kötelező a bejelentés, valamint a szervezetnek rendelkeznie kell a megfelelő kapacitásokkal a kockázatfelmérésre, az észlelésre és a válaszadásra.

Az Egyesült Államokban a szabályozás központi szereplője az FDA (Food and Drug Administration), amely több részletes iránymutatást dolgozott ki a BCI rendszerek kiberbiztonsági követelményeiről. A 2023-ban frissített Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions című dokumentum előírja, hogy a gyártóknak kötelező fenyegetettség elemzés, sebezhetőségkezelést és szoftver-ellátási lánc transzparenciát alkalmazniuk. Az FDA külön hangsúlyt fektet arra, hogy a gyártók Software Bill of Materials (SBOM) dokumentációt készítsenek, amely minden szoftverkomponenst és azok verzióját átláthatóan felsorolja. Emellett a Postmarket Management of Cybersecurity in Medical Devices útmutató a frissítési és hibakezelési folyamatok részletes követését és auditálását is előírja.

A BCI rendszerekre vonatkozó nemzetközi szabványok jelentős szerepet játszanak a megfelelőség biztosításában. Az ISO 13485:2016 szabvány a minőségirányítás alapjait fekteti le, míg az IEC 62304:2006 a szoftver-életciklus követelményeit definiálja. Ezek a szabványok megkövetelik a fejlesztéstől a karbantartásig tartó folyamatok dokumentálását és a biztonsági kockázatok következetes kontrollját. A kommunikációs csatornák védelmét az IEEE 802.15.6 szabvány szabályozza, amely testközeli hálózatok esetében is előírja a megfelelő titkosítási és hitelesítési mechanizmusok alkalmazását.

Az adatvédelmi megfelelőség különösen érzékeny kérdés, hiszen a BCI rendszerek által rögzített neurális mintázatok sokszor különleges személyes adatnak minősülnek. Az Európai Unióban a GDPR egyértelműen kimondja, hogy az egészségügyi vagy biometrikus adatok feldolgozásához kifejezett hozzájárulás szükséges, és a felhasználóknak joguk van a teljes körű tájékoztatáshoz a kezelés céljáról, módjáról és időtartamáról. Az Egyesült Államokban a HIPAA a személyazonosításra alkalmas egészségügyi adatok védelmét biztosítja, és kötelezővé teszi a hozzáférés-szabályozást, valamint az adatok titkosítását mind az adattárolás, mind az adatátvitel során.

A nemzetközi és hazai megfelelési követelmények egyre inkább egy irányba mutatnak: a BCI rendszerek fejlesztőinek és üzemeltetőinek olyan interdiszciplináris megközelítést kell alkalmazniuk, amely egyszerre foglalja magában a technológiai kockázatok mérséklését, az etikai felelősségvállalást, valamint a jogi követelmények teljesülését. A jogi környezet szigorodása és a társadalmi elvárások növekedése miatt minden fejlesztői és klinikai szereplő számára kulcskérdés, hogy a biztonsági protokollokat már a tervezési folyamat elejétől beépítse az eszköz életciklusába.

Sebezhetőségek és támadási lehetőségek BCI rendszerekben

Az agyba ültethető orvostechnikai eszközök a BCI rendszerek működése egy rendkívül összetett architektúrára épül, amely a biológiai idegrendszer és a digitális technológia határán helyezkedik el. Ezek az eszközök általában egy beültetett modulból, egy testfelszíni vagy testközeli kommunikációs interfészből, valamilyen feldolgozó és vezérlő szoftverből, valamint egy orvosi informatikai rendszerhez való integrációból állnak. A rendszer központi eleme az implantátum, amely közvetlenül kapcsolódik az idegszövethez, és szenzorok illetve stimulációs elektródák révén képes mérni és módosítani az agyi elektromos aktivitást. Az implantátumba épített mikrokontroller – a rajta futó firmware-rel együtt – gyakran valós idejű előfeldolgozást, adattömörítést vagy titkosítást végez, mielőtt az adatok továbbításra kerülnének a külső egység felé.

E technológiai komplexitás ugyanakkor példátlan sebezhetőségi mintázatot is eredményez, mivel a kiberbiztonsági incidensek hatása közvetlenül kiterjedhet a páciens neurológiai működésére, döntési képességére és pszichés állapotára. A fenyegetettségi térkép egyik legkritikusabb rétege a beágyazott firmware, amely gyakran aluldefiniált biztonsági kontrollokkal kerül ki a klinikai tesztelésre. A gyártók sok esetben a funkcionalitás gyors demonstrálására fókuszálnak, miközben háttérbe szorul a digitális aláírással történő verzióhitelesítés, a titkos kulcsok védelme, vagy a tanúsítványalapú szoftverellenőrzés. Egy olyan firmware, amely nem rendelkezik megbízható hitelesítési mechanizmussal, lehetővé teszi a támadók számára a módosított frissítések feltöltését, ezáltal backdoor-okat telepíthetnek, manipulálhatják a stimulációs paramétereket vagy titokban gyűjthetik a páciens neurális adatait. Mindez különösen kockázatos, mert a kompromittált működés gyakran észrevétlenül marad, és így a felhasználó nem érzékeli az eszköz viselkedésének megváltozását – miközben a támadás hatása akár mélyreható neurológiai torzulást is előidézhet.

A digitális kapcsolat elsődleges célja, hogy a neurológiai adatokat továbbítsa egy feldolgozó platformra, amely lehet mobilalkalmazás vagy akár felhőalapú tároló- és elemzőrendszer. Ezen a szinten a gyártók gyakran lehetőséget biztosítanak távfelügyeletre, konfiguráció módosítására, firmware-frissítések telepítésére, valamint prediktív karbantartásra. Éppen ezért az architektúrában rejlő kiberbiztonsági kockázatok több, egymásra épülő rétegben jelennek meg, és egyetlen gyenge pont is képes az egész rendszer kompromittálására.

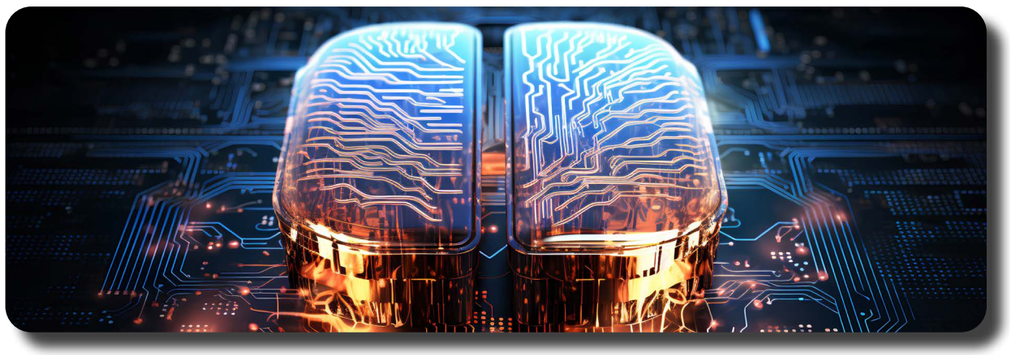
A sebezhetőségek egyik legsérülékenyebb pontját a vezeték nélküli kommunikációs csatornák jelentik. A gyártók jelentős része a kis fogyasztású rádiós protokollokra, például Bluetooth Low Energy vagy egyedi frekvenciás átviteli megoldásokra építi a távoli vezérlést és a monitorozást. Bár ezek a protokollok magas szintű mobilitást biztosítanak, a titkosítás és a hitelesítés megvalósítása sok esetben nem követi a kritikus infrastruktúrákra érvényes szabványokat. Ha a kommunikáció titkosítása gyenge, a támadó passzív módon lehallgathatja az adatokat, vagy aktív módon képes lehet visszajátszani korábban rögzített érvényes üzeneteket. A visszajátszás eredményeként a készülék téves parancsokat hajt végre, amelyek megváltoztathatják az idegi stimuláció intenzitását vagy teljesen leállíthatják a működést. A kutatások és a kísérleti támadások azt is igazolják, hogy a protokollok konfigurációs sebezhetősége – például egy gyenge párosítási folyamat vagy egy nem megfelelően védett diagnosztikai csatorna – ugyanúgy alkalmas a rendszer kompromittálására, mint a klasszikus szoftverhibák.

A jelfeldolgozó algoritmusok manipulációja egy viszonylag új és egyre nagyobb figyelmet kapó fenyegetési forma. A támadók célzottan olyan inputokat generálhatnak – például modulált elektromágneses jeleket vagy ultrahangos impulzusokat –, amelyek befolyásolják a szenzorok mérési eredményeit. A BCI eszközök neurális adatfeldolgozása sok esetben gépi tanulásra vagy adaptív szűrési algoritmusokra épül, és a támadó képes lehet speciálisan megtervezett mintázatokkal a döntéshozatalt torzítani. Az így létrejövő torzítás nem feltétlenül jár azonnali észrevehető tünetekkel, ezért különösen veszélyes, ha a készülék hosszabb időn át dolgozik téves adatokkal. Az ehhez hasonló támadások – amelyeket gyakran a mesterséges intelligencia adverzáriális sérülékenységeihez hasonlítanak – a közeljövőben egyre szélesebb körben válhatnak realitássá, főként ha a gyártók nem végeznek alapos szcenárióalapú tesztelést.

Nem hagyhatók figyelmen kívül a fizikai támadások sem, még ha ritkábban fordulnak is elő. Ha a támadó közvetlen hozzáférést szerez a külső kommunikációs modulhoz, lehetősége nyílik oldalcsatornás visszafejtési eljárások alkalmazására. A memória dumpolása, az energiafogyasztási profil elemzése vagy az elektromágneses szivárgások megfigyelése révén rekonstruálhatók a készülék titkos kulcsai és a konfigurációs beállításai. Mivel az orvosi környezetben a testközeli egységek nem minden esetben rendelkeznek megfelelő fizikai védelmi rétegekkel, ezek a támadások célzott helyzetekben reális fenyegetést jelenthetnek.

Különösen aggasztó az a tendencia, hogy a neurális spoofing technikák és a felhőalapú adminisztrációs rendszerek sebezhetősége együttesen képes a teljes rendszer feletti irányítás megszerzéséhez vezetni. A neurális spoofing során a támadó nem csupán a szenzoradatokat módosítja, hanem a konfigurációs protokollt is manipulálja, így képes legitim parancsok szimulálására és a felhasználó megtévesztésére. Ezzel párhuzamosan a felhőalapú platformokon történő adatelemzés, firmware-verziókezelés és hozzáférés-adminisztráció szintén számos támadási pontot hordoz, amelyek kihasználása esetén egy támadó távolról új firmware-verziókat telepíthet, neurális adatokat szivárogtathat vagy teljes hozzáférést nyerhet a páciens eszközéhez.

A BCI rendszerek támadási felülete lényegesen szélesebb, mint a hagyományos orvostechnikai eszközöké, mivel nem csupán az életfunkciókat, hanem a felhasználó gondolati folyamatait, döntéshozatalát és érzékelését is képesek befolyásolni. E komplexitás következtében a sebezhetőségek technikai, biológiai és pszichológiai síkokon fonódnak össze, így minden támadási lehetőség potenciálisan súlyos egészségügyi és adatvédelmi incidenst eredményezhet.



A védelmi stratégiának az architektúra minden rétegét át kell fognia: a hardveres hitelesítéstől és a biztonságos firmware-verifikációtól kezdve a kriptográfiai kulcsmenedzsmenten és a szoftverfrissítési láncon át a felhőalapú adatfeldolgozás hozzáférés-szabályozásáig. Egyetlen komponens hibája vagy hiányzó biztonsági kontrollja dominóhatást válthat ki, amely a felhasználó fizikai épségét és neurális adatainak biztonságát is veszélybe sodorja. Éppen ezért a gyártóknak és egészségügyi szolgáltatóknak nem elegendő a klasszikus információbiztonsági gyakorlatokra hagyatkozni, hanem olyan komplex kockázatkezelési szemléletet kell alkalmazniuk, amely figyelembe veszi a neurális interfészek sajátos sérülékenységeit a teljes életciklus során – a tervezéstől a karbantartásig.

Kiemelt kiberbiztonsági kihívások agyi interfészeknél

Az agy-számítógép interfészek és a beültethető neuromodulációs rendszerek sajátos kiberbiztonsági kockázatai olyan komplexitást hordoznak, amely messze túlmutat a hagyományos orvostechnikai eszközök kihívásain. Ezek az eszközök ugyanis nemcsak érzékeny személyes vagy egészségügyi adatokat kezelnek, hanem közvetlen beavatkozást biztosítanak az idegrendszer elektromos működésébe, így a kompromittálásuk fizikai, pszichológiai és jogi szempontból egyaránt súlyos következményekkel járhat. A biztonsági kihívások egy jelentős része abból fakad, hogy a gyártási és fejlesztési fázisok során a funkcionalitás és a klinikai hatékonyság élvez elsőbbséget, míg a kiberbiztonsági kontrollok integrációja sokszor csak később, a szabályozási megfelelés kényszeréből történik meg.

A legkritikusabb terület az integritás- és hitelességvédelem, amely a neurális jelek sértetlenségének és a rendszer által végrehajtott parancsok valódiságának biztosítását célozza. Ha egy támadó képes akár részlegesen módosítani az adatfolyamot, a készülék olyan parancsot hajthat végre, amely ellentétes a terápiás céllal, vagy közvetlen neurológiai károsodást okoz. Az integritás sérülése ráadásul szoros összefüggésben áll az adatok hitelességének elvesztésével, mivel a felhasználó és az orvosi személyzet nem képes megkülönböztetni a legitim üzenetet a támadó által generált vagy módosított parancstól.

A helyzetet súlyosbítja, hogy a BCI eszközök működésében a szenzoradatok és a stimulációs utasítások valós idejű ciklusban követik egymást, ezért minden támadási beavatkozás a gyakorlatban másodpercek alatt idézhet elő klinikai hatást.

A másik kiemelt kockázati dimenzió a rendelkezésre állás biztosítása, amely különösen fontos a létfontosságú funkciókat támogató implantátumoknál, például mélyagyi stimulátoroknál vagy agyi jelfeldolgozással vezérelt protéziseknél. Egy célzott túlterheléses támadás (Denial of Service) a rádiós kommunikáció megszakításával vagy a firmware memóriájának szándékos túlterhelésével képes lehet a rendszer működését részlegesen vagy teljesen blokkolni. Mivel az eszközök egy része automatikus védelmi mechanizmust alkalmaz, amely a rendellenességet érzékelve kikapcsolja a stimulációt, a támadás közvetlenül a beteg motoros funkcióinak, kognitív képességeinek vagy életminőségének romlásához vezethet. A DoS típusú fenyegetések másik formája az, amikor a támadó szándékosan téves állapotjelentéseket küld, amelyek alapján a kezelő szoftver a készüléket biztonsági üzemmódba kapcsolja, gyakorlatilag feleslegesen blokkolva a működését.

A neurális adatok sajátossága miatt rendkívül magas a privát információk szivárgásának kockázata is. Az implantátumok által gyűjtött és továbbított jelek között olyan mintázatok találhatók, amelyek részben vagy egészben alkalmasak lehetnek a felhasználó személyazonosságának, mentális állapotának, esetenként a gondolati tartalmainak vagy reakcióinak visszakövetésére. Ez a tulajdonság önmagában megkülönbözteti a BCI rendszereket más szenzoros egészségügyi eszközöktől. Egy sikeres adatlopás tehát nem pusztán technikai incidensnek minősül, hanem súlyosan érintheti a felhasználó méltóságát és autonómiáját, valamint kiterjedt jogi következményekkel járhat a személyes adatok védelmére vonatkozó szabályozások – például a GDPR vagy a HIPAA – alapján. A támadó ráadásul a neurális mintázatokkal visszaélve képes lehet profilalkotásra, amely sérti az egyén önrendelkezését, és új szintre emeli a magánszféra sérülésének mértékét.

A jogi és etikai kontextusban a BCI rendszerek kiberbiztonsági incidensei súlyosabb következményekkel bírnak, mint a klasszikus orvostechnikai eszközök hibái. Az autonómia és a beleegyezés kérdése kifejezetten kényes, mivel a felhasználók többsége nincs felkészülve annak megértésére, hogy a neurális adatok manipulálása miként hat vissza a saját döntéshozatalukra és önérzékelésükre. Egy támadás esetén a károk felmérése és a helyreállítás sokkal összetettebb, hiszen a hardveres vagy szoftveres újratelepítés önmagában nem feltétlenül elegendő a neurális következmények megszüntetéséhez.

Az itt megjelenő kiberbiztonsági kihívások minden szinten interdiszciplináris megközelítést igényelnek, ahol a szoftvermérnöki gyakorlat, a neurológiai szakértelem és a szigorú jogi megfelelés egyaránt nélkülözhetetlen. Az a gyártó, aki ezeket a szempontokat nem integrálja már a tervezési folyamat kezdetétől, lényegében lehetőséget ad olyan fenyegetési forgatókönyvek kialakulására, amelyek súlyosan veszélyeztethetik a felhasználó testi integritását és emberi méltóságát.

Biztonsági architektúrák és védelmi megközelítések

A BCI rendszerek és agyba ültethető neuromodulációs eszközök kiberbiztonságának megtervezése során különösen nagy jelentősége van annak, hogy a védelem minden réteget együttesen fedjen le. Ez a többdimenziós megközelítés magában foglalja a hardverszintű védelem, a szoftveres hitelesítés, a titkosítás és a biztonságos frissítés komplex rendszerét.

A biztonsági architektúra első kritikus eleme a kriptográfiai védelem, amelynek célja, hogy a neurális adatforgalom és a konfigurációs parancsok illetéktelen hozzáférés vagy módosítás ellen védettek legyenek. A jelenleg leginkább ajánlott gyakorlat a modern, jól audittált algoritmusok alkalmazása, mint például az AES-256 titkosítás a vezeték nélküli kommunikációban és az elliptikus görbe alapú kulcscsere protokollok a párosítási folyamat során. A kulcsmenedzsment elengedhetetlen része a rendszer biztonságának, mert ha a titkos kulcsok előre definiáltak vagy minden eszközön azonosak, egyetlen kompromittált eszköz elegendő lehet a teljes gyártói ökoszisztéma támadhatóságához.

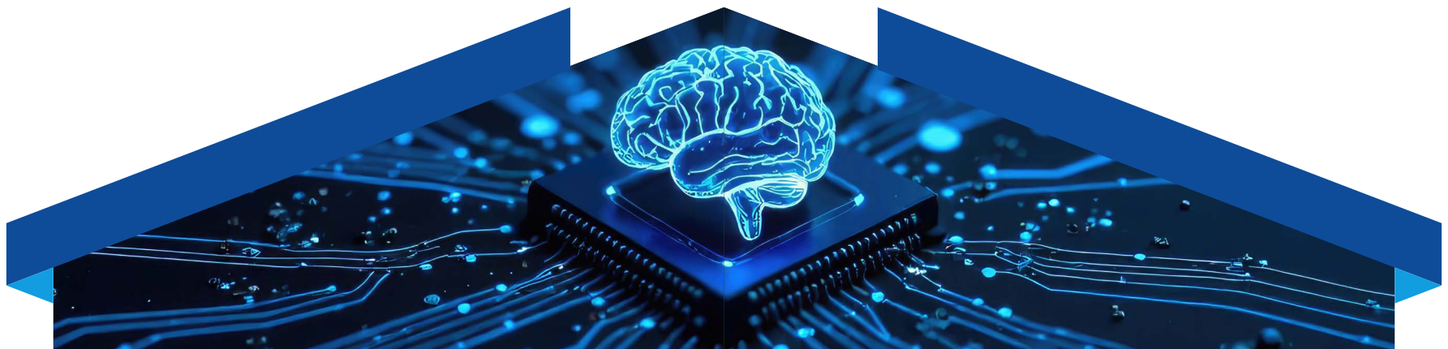
A hardverszintű védelem kiterjed a fizikai hozzáférés elleni védekezésre, például a debug interfészek inaktiválására, a memória olvasásvédelmére és a szenzorok elektromágneses árnyékolására. Ezek a megoldások azért különösen fontosak, mert a fizikai visszafejtési technikák – például a memória dumpolás vagy a side-channel elemzés – már laboratóriumi környezetben bizonyítottan képesek a kulcsok rekonstruálására és a firmware állomány visszanyerésére. A biztonsági architektúrában alapvető szerepet kap az is, hogy az implantátum vezérlőmodulja képes legyen minden kommunikációs kísérletet naplózni és a szokatlan aktivitásról riasztást küldeni a kezelő felületre.

A szoftveres védelmi réteg egyik legfontosabb komponense a digitális aláíráson alapuló firmware-verifikáció, amely lehetővé teszi, hogy az eszköz kizárólag a gyártó által hitelesített és változatlan frissítéseket fogadjon el. Ez a mechanizmus egyaránt védi a felhasználót a rosszindulatú támadásoktól és a nem szándékos konfigurációs hibáktól. A firmware-aláírási eljárások bevezetését azonban sok esetben nehezíti a beültetett eszközök korlátozott számítási kapacitása és az energiafogyasztás minimalizálásának kényszere. A legújabb fejlesztések olyan optimalizált aláírás-ellenőrzési algoritmusok alkalmazását célozzák, amelyek kis energiaigénnyel is képesek gyors ellenőrzést biztosítani, így a beteg biztonsága nem kerül szembe a praktikus üzemidő elvárásával.

A frissítési mechanizmusok önálló támadási felületet alkotnak, ezért a biztonsági architektúrának szigorúan szabályozott folyamatokat kell definiálnia a verziók kezelésére. A fejlettebb rendszerek felügyelt frissítési modellt használnak, amelyben minden firmware-frissítést előzetes jóváhagyási lépés és többtényezős hitelesítés előz meg. Ez a modell általában felhasználói azonosítást, gyártói tanúsítványalapú hitelesítést és időbélyegzéssel ellátott naplózást egyaránt alkalmaz. A védelmi stratégiában fontos szerepet játszik a frissítési folyamat integritásának folyamatos ellenőrzése is, hiszen a támadók előszeretettel élnek vissza a karbantartási rutinok során fellépő figyelmetlenségekkel vagy a szoftver-ellátási lánc hiányosságaival.

A biztonsági architektúra kialakításánál egyre több gyártó fordít figyelmet a gépi tanulás alapú anomália-észlelésre. A prediktív monitorozó rendszerek képesek automatikusan felismerni a szokatlan mintázatokat, például a túlzott kommunikációs aktivitást, az érvénytelen parancsismétlést vagy a neurális szenzorok jeleiben megjelenő torzításokat. Bár ezek a módszerek még gyermekcipőben járnak, az előzetes eredmények azt mutatják, hogy képesek lehetnek a korai támadásészlelésre és a gyors beavatkozás előkészítésére. E fejlesztések egyben új kihívásokat is teremtenek, hiszen a gépi tanulási modelleket magukat is fel kell készíteni az adverzáriális példák elleni védekezésre, hogy a támadó ne tudja őket félrevezetni speciális inputokkal.

A védelmi megközelítésekben központi elvként érvényesül a „defense in depth" szemlélet, amely szerint egyetlen biztonsági kontroll önmagában soha nem tekinthető elegendőnek. Csak akkor beszélhetünk viszonylagos biztonságról, ha a rétegezett védelem konzisztens módon kiterjed a hardverre, a firmware-re, a kommunikációs protokollokra és a felhőalapú adminisztrációs felületekre egyaránt. Ebben a környezetben minden hiányzó vagy gyenge láncszem a támadó számára potenciális beavatkozási pontot jelent, ami a BCI-k esetében nem csupán adatvesztést vagy szolgáltatáskimaradást, hanem tényleges neurológiai kockázatot idézhet elő.



Jogi és etikai megfontolások

A BCI rendszerek és az agyba ültethető neuromodulációs eszközök jogi és etikai megítélése egyedülálló kihívás elé állítja a szabályozó hatóságokat, a gyártókat és a kezelőorvosokat. Míg a hagyományos orvostechnikai eszközök esetében a kockázatok elsősorban fizikai síkon jelentkeznek, ezeknél a technológiáknál a fenyegetések átnyúlnak a mentális autonómia, az önrendelkezés, valamint az adatvédelmi jogok területére.

A jogi megfelelés egyik legfontosabb dimenziója a beleegyezés és informált hozzájárulás kérdése, amely sokkal komplexebb, mint egy hagyományos beavatkozás esetében. Egy BCI rendszer telepítésénél a páciensnek nemcsak azt kell megértenie, milyen élettani kockázatokkal jár az implantáció, hanem azt is, hogy a készülék idegi aktivitást gyűjt és továbbít, és a jövőben potenciálisan alkalmas lehet mentális állapotok befolyásolására. A jogszabályi környezet ugyan előírja az informált hozzájárulás követelményét, de a valóságban a legtöbb beteg számára a neurális adatok kiberbiztonsági aspektusai nem átláthatók, így a hozzájárulás sok esetben inkább formális, mint ténylegesen tudatos döntés eredménye.

Az autonómia és a beavatkozás dilemmája különösen akkor válik élessé, ha a rendszer működéséhez elengedhetetlen a felhőalapú adattárolás vagy a távoli konfigurációs lehetőség. Egyre gyakoribb, hogy a gyártó fenntartja magának a jogot a firmware frissítésére és a működési paraméterek módosítására, miközben a páciensnek nincs lehetősége a folyamat ellenőrzésére vagy megakadályozására. Ez a gyakorlat felveti a kérdést, hogy milyen mértékben mondhat le egy személy az önrendelkezéséről, amikor egy olyan rendszer mellett dönt, amely – akár jó szándékkal is – automatizáltan avatkozik be az idegrendszeri működésbe. A jogalkotás jelenlegi formájában nem ad egyértelmű választ arra, hogy ilyen esetben ki viseli a felelősséget, ha a firmware-frissítés következtében káros hatás vagy adatvesztés történik.

A BCI technológiákhoz kapcsolódó adatvédelmi és személyiségi jogi kockázatok is egyedülálló súlyúak. Az Európai Unióban a GDPR rendelkezései szerint a neurális adatok különleges kategóriába tartoznak, amelyre a legszigorúbb védelmi előírások érvényesek. Az Egyesült Államokban a HIPAA biztosítja az egészségügyi adatok védelmét, de a jogértelmezés még vitatott abban a kérdésben, hogy a gondolati folyamatokat tükröző jelek a személyes egészségügyi adatok körébe tartoznak-e. A szabályozási bizonytalanságot súlyosbítja, hogy a neurális adatok egy részéből pszichológiai profilok, preferenciarendszerek vagy akár politikai meggyőződések is visszakövetkeztethetők, ami a személyes autonómia megsértésének kiemelkedően érzékeny formáját jelenti.

Etikai szempontból különösen aggasztó a lehetősége annak, hogy a BCI eszközök működése révén egy harmadik fél – például a gyártó vagy egy támadó – képes lehet mentális állapotváltozást kiváltani, vagy szándékosan olyan stimulációs mintázatokat alkalmazni, amelyek megváltoztatják a felhasználó döntéshozatali mechanizmusát. Az orvosi etika hagyományos elvei, mint az „ártalmatlanság elve" és a „célhoz kötöttség", ebben a környezetben újraértelmezést igényelnek, mivel a technológia potenciálisan túlléphet a terápiás célt szolgáló alkalmazáson, és akár manipulatív eszközzé is válhat.

A jogi felelősség megoszlása sem egyértelmű, különösen a szoftver-ellátási lánc sérülékenységei esetében. Ha egy támadó egy beszállító cég alrendszerét kompromittálja, a felelősség a gyártót, az egészségügyi szolgáltatót és a szoftverfejlesztőt egyaránt érintheti. E problémakör miatt a kockázatmegosztási és felelősségbiztosítási modellek átdolgozása elkerülhetetlen.

A nemzetközi harmonizáció problémája is kiemelkedő jelentőségű, hiszen a gyártók globális piacon értékesítik termékeiket, miközben a jogi és etikai követelmények országonként jelentősen eltérnek. Nincs olyan egységes protokoll vagy szabályrendszer, amely mindenhol egyformán meghatározná a neurális adatok védelmének minimumszintjét vagy a BCI működésének etikai korlátait. Ez a széttagoltság egyaránt nehezíti a szabályozói felügyeletet és a páciensek tájékoztatását, miközben a támadók számára kihasználható kiskapukat teremt.

Esettanulmányok – Gyakorlati példák

A BCI rendszerek és az agyba ültethető neuromodulációs eszközök kiberbiztonsági és etikai kockázatai nem csupán elméleti kérdések. Az elmúlt évek során több olyan eset is ismertté vált, amelyek jól mutatják, milyen következményekkel járhat, ha a fejlesztés, üzemeltetés vagy klinikai kutatás során a biztonsági szempontok háttérbe szorulnak.

Neuralink

A nemzetközi gyakorlat egyik legismertebb példája a Neuralink pilotprogram, amelynek célja olyan agyba ültethető modulok fejlesztése volt, amelyek vezeték nélküli kapcsolaton keresztül, valós idejű kommunikációra képesek külső eszközökkel. Bár a projekt komoly idegtudományi és mérnöki eredményeket ért el, számos szakértő bírálta a kiberbiztonsági megfontolások átláthatóságának hiányát. Több biztonsági kutató felhívta a figyelmet arra, hogy a kommunikációs protokollok dokumentációja nem tartalmazott részletes információt a titkosítási és hitelesítési eljárásokról, és nem volt bizonyítható, hogy a firmware-frissítéseket minden esetben digitális aláírás védi. Bár bizonyított támadás ebben az időszakban nem történt, a projekt jól példázta, mennyire sérülékeny lehet egy nagy figyelemmel kísért fejlesztés, ha a biztonsági és klinikai validációs szempontok nincsenek összehangolva.

Cochlear Ltd.

Egy másik fontos nemzetközi tapasztalatot a Cochlear Ltd. eszközeinek sebezhetősége szolgáltatta, amelyek hallásjavító implantátumként működnek, de számos technológiai rokonságot mutatnak a BCI rendszerekkel. Kutatók laboratóriumi környezetben demonstrálták, hogy a vezeték nélküli kommunikáció lehallgatásával és manipulálásával távoli parancsvégrehajtás végezhető. A támadók képesek voltak a készülék konfigurációját módosítani, illetve olyan zajimpulzusokat generálni, amelyek ideiglenes halláskárosodást idézhettek elő. Az eset bizonyította, hogy valós idejű támadás klinikai környezetben is kivitelezhető, ha a protokollok és a kulcsmenedzsment hiányos.

Egy korai, kevésbé ismert eset, amikor a kutatók egy BCI prototípus adverzáriális inputokkal történő manipulációját demonstrálták. A kísérlet során mesterséges rádiójelek segítségével a neurális jelfeldolgozót téves döntésekre késztették, ami a rendszer automatikus stimulációs válaszait hibás paraméterek alapján indította el. Bár a projektet kontrollált környezetben hajtották végre, a tanulmány megmutatta, hogy a gépi tanuláson alapuló jelfeldolgozás manipulálhatósága reális fenyegetést jelent.

Medtronic

A nemzetközi incidensek közül kiemelkedik a Medtronic implantálható neurostimulátorok sérülékenysége, amelyet a 2018–2019-es biztonsági auditok során tártak fel. Az FDA által is elismert kockázat lényege az volt, hogy a készülékek vezeték nélküli programozási protokollja hitelesítetlen parancsok fogadására alkalmas volt. Egy támadó viszonylag egyszerű eszközökkel képes lehetett volna a stimuláció intenzitását módosítani vagy a készülék működését leállítani, ami életveszélyes állapotok kialakulásához vezethetett volna. Az ügy nyomán a gyártó firmware-frissítéseket adott ki, és szigorította a hozzáférési szabályokat.

A Medtronic által használt, beágyazott rendszerekben alkalmazott VxWorks operációs rendszer hét kritikus sebezhetőséget tartalmazott (URGENT/11 néven), amelyek távoli kódfuttatást és szolgáltatásmegtagadást is lehetővé tehettek. Bár közvetlen támadás nem történt, az FDA és a CISA figyelmeztetést adott ki, mivel az érintett eszközök sérülékenyek lehettek. A Medtronic a gyártásban lévő eszközök szoftverfrissítésével és hálózati védekezéssel reagált az incidensre.

Biztonsági kutatók három súlyos sebezhetőséget tártak fel a Medtronic MyCareLink Smart betegolvasó eszközeiben, amelyek Bluetooth-on keresztül lehetővé tették az illetéktelen kódbevitel és firmware-manipuláció lehetőségét. A sebezhetőségek közé tartozott hitelesítés megkerülése, heap túlcsordulás és a digitális aláírás nélküli frissítések feltöltése. Bár a támadásokhoz fizikai közelség kellett, az FDA és a Medtronic közös közleményben ismerte el a problémát, és sürgős frissítést kezdeményeztek.

Az FDA hivatalosan is visszahívta a Medtronic MiniMed 508 és Paradigm sorozatú inzulinpumpáit, miután kiderült, hogy a vezeték nélküli kommunikáció titkosítási hiányosságai lehetővé tehetik az adagolási beállítások távoli módosítását. Noha nem észleltek aktív támadásokat, a biztonsági kockázat súlyossága miatt a Medtronic több ezer eszköz cseréjét javasolta. A hatóság szerint a sebezhetőség különösen veszélyes lehetett volna, mivel inzulin túladagolást is okozhatott volna.

Egy nemzetközi kutatócsoport demonstrálta, hogy EEG-alapú agy–számítógép interfészekkel (pl. Emotiv Epoc headset) lehetséges személyes adatok kinyerése pusztán az agyi válaszok (P300 hullámok) elemzésével. A vizsgálatokban a felhasználók vizuális ingerekre reagáltak, miközben a rendszer az agyhullámok alapján képes volt kikövetkeztetni PIN-kódok számjegyeit, születési hónapot vagy lakhelyet. A tanulmány először mutatott rá, hogy akár kereskedelmi EEG-fejhallgatók is hordozhatnak adatszivárgási kockázatot.

A Black Hat USA 2017 konferencián Billy Rios és Jonathan Butts biztonsági kutatók bemutatták, hogy a Medtronic bizonyos pacemakerei és programozóeszközei mennyire sebezhetőek lehetnek célzott malware-támadásokkal szemben. A bemutatóban sikerült rosszindulatú firmware-t telepíteni egy programozóeszközre, amellyel ezután az implantátum működése is manipulálhatóvá vált volna. Bár valós betegkárosodás nem történt, az eset felhívta a figyelmet a beültethető eszközök kiberbiztonságának kritikus fontosságára.

A teljes előadás visszanézhető az alábbi linkre kattintva.

A felsorolt esetek világosan mutatják, hogy a fejlesztési környezet, a klinikai kutatás és a piaci forgalmazás során egyaránt fennáll a veszélye annak, hogy a titkosítás, a firmware-verifikáció, a hozzáférés-szabályozás és az adatvédelmi folyamatok nem megfelelően illeszkednek össze. Mindez olyan sebezhetőségi láncot hoz létre, amely a támadók számára kaput nyit a rendszer és a felhasználó idegrendszere felé.

Jövőbeli trendek és szabályozási irányok

A BCI rendszerek és az agyba ültethető orvostechnikai implantátumok fejlődése az elkövetkező években várhatóan még gyorsabb ütemre kapcsol, ami újabb, eddig nem tapasztalt kiberbiztonsági és jogi kihívásokat teremt. A technológiai trendek egyik legmarkánsabb iránya a mesterséges intelligencia szoros integrációja, amely nemcsak a jelfeldolgozást, hanem a valós idejű döntéstámogatást is automatizálni fogja. A prediktív modellek képesek lesznek előre jelezni a beteg állapotváltozását vagy a stimuláció hatékonyságát, ám ezzel párhuzamosan megjelenik a gépi tanulási algoritmusok manipulációjának veszélye. Az adverzáriális inputok elleni védekezés jelenleg még nem megoldott, így reális kockázatot jelent, hogy egy támadó célzott mintázatokkal torzítsa a modell döntéseit.

A fejlődő trendek közé tartozik a felhőalapú és edge computing platformok elterjedése, amelyek az adattárolás és feldolgozás rugalmasságát növelik, ugyanakkor szélesítik a támadási felületet. Az eszközök egyre nagyobb arányban kapcsolódnak közvetlenül internetes infrastruktúrához, amelyen keresztül távoli firmware-frissítés, konfiguráció-módosítás és jelfeldolgozás történik. Ez a működési modell különösen érzékeny a szolgáltatásmegtagadásos támadásokra, a jogosulatlan hozzáférésre, valamint a láncolt ellátási lánc sebezhetőségeire.

A jövőben a gyártóknak és szolgáltatóknak várhatóan kötelező lesz részletes Software Bill of Materials (SBOM) dokumentációt biztosítaniuk, amely pontosan nyilvántartja a komponensek eredetét és verzióját, ezzel segítve a gyors reakciót sérülékenységek felmerülésekor.

Szabályozási szempontból a következő években valószínűsíthető a jogszabályok szigorítása, különösen az adatvédelmi megfelelés és az életbiztonsági kockázatok kezelése területén. Az Európai Unió a Medical Device Regulation (MDR) mellett egyre inkább integrálja a NIS2 irányelv kockázatkezelési szemléletét, amely szigorúbb kötelezettségeket ró a gyártókra a hálózati és információs rendszerek védelme terén. Az Egyesült Államokban az FDA szintén továbbfejleszti a Cybersecurity in Medical Devices irányelveit, várhatóan kötelező érvényűvé téve az éles működés közbeni eseménynaplózást és a távfelügyeleti hozzáférés erős hitelesítését. Mivel a BCI eszközök különösen érzékeny személyes adatokat kezelnek, előrevetíthető, hogy a GDPR és a hasonló nemzeti szabályozások kiterjesztett hatálya alá kerülnek, és a neurális adatok kezelésére külön kategóriák jönnek létre.

Technológiai szinten a gyártók középtávon várhatóan nagyobb hangsúlyt helyeznek majd az ellenállóképesség (resilience) biztosítására, vagyis arra, hogy a rendszerek részleges kompromittálódás esetén is képesek legyenek minimális működés fenntartására. A hardver-szoftver architektúrákban megjelenhetnek a zero trust modell elemei, ahol minden kommunikációs és konfigurációs művelet explicit hitelesítést és titkosítást igényel, függetlenül attól, hogy a művelet a felhasználó közvetlen környezetéből indul-e. Ez a szemlélet kulcsszerepet kaphat a jövő BCI biztonsági tervezésében, mivel egyre gyakoribbak lesznek a távoli támadások és ellátási lánc kompromittációk.

Mindezek a trendek világosan mutatják, hogy a BCI rendszerek kiberbiztonsága és szabályozása a következő években új fejezetbe lép. A technológiai lehetőségek bővülése nemcsak klinikai előnyöket hoz, hanem példátlan mértékű adatvédelmi és etikai kockázatot is, amelyre a fejlesztőknek, szabályozóknak és egészségügyi intézményeknek egyaránt fel kell készülniük.

Összefoglaló

Az agyba ültethető orvostechnikai eszközök és a BCI rendszerek fejlődése az egészségügyi technológia egyik legdinamikusabb területévé vált, miközben a kiberbiztonsági, adatvédelmi és etikai követelmények példátlan kihívások elé állítják a fejlesztőket, klinikai kutatókat és szabályozókat. A vizsgálat egyértelműen rámutatott, hogy ezek az eszközök egyedi módon egyesítik a klasszikus számítástechnikai fenyegetettséget a közvetlen biológiai és pszichológiai következményekkel, így a kompromittálás kockázata messze meghaladja a hagyományos digitális eszközök kockázati szintjét.

A tanulmány feltérképezte azokat a sebezhetőségeket, amelyek a firmware-ben, a vezeték nélküli kommunikációban, a jelfeldolgozó algoritmusokban és a felhőalapú adminisztrációs rendszerekben egyaránt megjelennek. A konkrét esettanulmányok – köztük a Medtronic és Cochlear Ltd. incidensei – egyértelműen bizonyítják, hogy a titkosítás hiánya, a nem megfelelő hitelesítési mechanizmusok és a hozzáférés-szabályozás hibái súlyos adatvédelmi és egészségügyi következményekkel járhatnak.

A jogi környezet vizsgálata feltárta, hogy a meglévő szabályozások – például az MDR, a GDPR, illetve az FDA irányelvei – részletes kereteket kínálnak, de sok területen még mindig nem adnak egyértelmű választ a felelősség, az autonóm döntéshozatal és az adatkezelés pontos határaira. Az etikai megfontolások különösen érzékeny kérdéssé váltak, hiszen a neurális adatok kezelése és a stimulációs protokollok módosítása közvetlenül érintheti a felhasználó mentális autonómiáját, önérzékelését és személyiségi jogait.

A technológiai trendek elemzése világossá tette, hogy a következő években az AI-integráció, a felhőalapú adattárolás és a zero trust biztonsági modellek elterjedése új kockázati dimenziókat nyit meg. A jövő kulcskérdése az lesz, miként lehet egyensúlyt teremteni a terápiás hatékonyság, az adatbiztonság és az etikai normák között.

Összességében a BCI rendszerek kiberbiztonsága nem kezelhető elszigetelt technológiai problémaként. Csak akkor biztosítható a páciensek védelme, ha a gyártók már a fejlesztés első lépésétől alkalmazzák a beépített biztonság (security by design) elvét, a szabályozók folyamatosan frissítik a megfelelőségi követelményeket, és az egészségügyi szolgáltatók a gyakorlatban is következetesen betartják a kockázatcsökkentési protokollokat. Azok az ökoszisztémák, amelyek nem rendelkeznek átlátható kulcsmenedzsmenttel, naprakész firmware-verifikációval, valamint robusztus hozzáférés-szabályozással, elkerülhetetlenül célponttá válnak egy olyan világban, ahol a neurális adatok értéke és érzékenysége soha nem látott szintre emelkedik.

A témában készült podcast adásunkat meghallgathatja az alábbi linkre kattintva.

Források

- **CybSafe.** (2022) *Human Factors in Cyber Security: Understanding People's Part in Security and Protection.* https://www.cybsafe.com/resources/human-factors-in-cyber-security/ (Letöltve: 2025. június 28.)
- **IEEE.** (2012) *IEEE Standard for Local and Metropolitan Area Networks – Part 15.6: Wireless Body Area Networks.* https://standards.ieee.org/standard/802_15_6-2012.html (Letöltve: 2025. június 25.)
- **ISO.** (2016) *ISO 13485:2016 – Medical Devices Quality Management Systems – Requirements for Regulatory Purposes.* https://www.iso.org/standard/59752.html (Letöltve: 2025. június 28.)
- **Unite.AI.** (2024) *Empathetic AI: Transforming Mental Healthcare and Beyond with Emotional Intelligence.* https://www.unite.ai/empathetic-ai-transforming-mental-healthcare-and-beyond-with-emotional-intelligence/ (Letöltve: 2025. június 30.)
- **World Health Organization (WHO).** (2022) *Ethics and Governance of Artificial Intelligence for Health.* https://www.who.int/publications/i/item/9789240029200 (Letöltve: 2025. június 28.)

- **arXiv.** (2022) *Adversarial Attacks on EEG-Based Brain-Computer Interfaces.* https://arxiv.org/pdf/2205.00893 (Letöltve: 2025. július 8.)
- **arXiv.** (2024) *A Survey on Brain-Computer Interface Cybersecurity.* https://arxiv.org/html/2412.07231v1 (Letöltve: 2025. július 29.)
- **CISA.** (2018). *ICS Medical Advisory (ICSMA-18-058-01).* https://www.cisa.gov/news-events/ics-medical-advisories/icsma-18-058-01 (Letöltve: 2025. július 14.)
- **Compass IT Compliance.** (n.d.) *Can Neuralink Be Hacked? Cybersecurity Experts Discuss Potential Risks.* https://www.compassitc.com/blog/can-neuralink-be-hacked-cybersecurity-experts-discuss-potential-risks (Letöltve: 2025. július 11.)
- **EUR-Lex.** (2024) *Regulation (EU) 2024/2847 on Artificial Intelligence.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847 (Letöltve: 2025. július 1.)
- **European Commission.** (2022) *Cybersecurity of Medical Devices.* https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf (Letöltve: 2025. július 9.)
- **FDA.** (2019) *Cybersecurity Vulnerabilities Identified in Medtronic Cardiac Devices.* https://www.fda.gov/media/119933/download (Letöltve: 2025. július 15.)
- **IEEE.** (2024) *Adversarial Attacks and Defenses in EEG-Based Brain-Computer Interfaces.* https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10887386 (Letöltve: 2025. július 3.)
- **IEEE.** (2023) *A Security Model for Neural Interface Devices.* https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10577965 (Letöltve: 2025. július 22.)
- **JSTOR.** (2012) *Ethical Implications of Brain-Machine Interfaces.* https://www.jstor.org/stable/43593914 (Letöltve: 2025. július 2.)
- **MDPI.** (2021) *Wearable EEG-Based BCI Systems: A Review.* **https://** www.mdpi.com/1424-8220/21/20/6886 (Letöltve: 2025. július 30.)
- **Medtronic.** (2024) *URGENT/11 Vulnerabilities.* https://global.medtronic.com/xg-en/product-security/security-bulletins/urgent-11-vulnerabilities.html (Letöltve: 2025. július 25.)
- **Nature.** (2024) *Neural Data Integrity in BCI Systems.* https://www.nature.com/articles/s41598-024-58535-4 (Letöltve: 2025. július 5.)
- **NCBI.** (2021) *Brain–Computer Interface: A Review on Signal Processing Techniques.* https://pmc.ncbi.nlm.nih.gov/articles/PMC8288388/ (Letöltve: 2025. július 23.)
- **NCBI.** (2023) *Cyber Risks in Closed-Loop Neurotechnology.* https://pmc.ncbi.nlm.nih.gov/articles/PMC10403483/ (Letöltve: 2025. július 18.)
- **NCBI.** (2020) *Cybersecurity Challenges in Connected Medical Devices.* https://pmc.ncbi.nlm.nih.gov/articles/PMC6955451 (Letöltve: 2025. július 4.)
- **OpenReview.** (2020) *Practical Adversarial Attacks on Brain–ComputerInterfaces.* https://openreview.net/forum?id=0sEIBFb4cs (Letöltve: 2025. július 17.)
- **ResearchGate.** (2016) *Brainjacking: Implant Security Issues in Invasive Neuromodulation.* https://www.researchgate.net/publication/303094988_Brainjacking_Implant_Security_Issues_in_Invasive_Neuromodulation (Letöltve: 2025. július 24.)

- **ResearchGate.** (2024) *Cybersecurity Issues in Brain–Computer Interfaces: Analysis of Existing Bluetooth Vulnerabilities.* https://www.researchgate.net/publication/382165496_Cybersecurity_Issues_in_Brain-Computer_Interfaces_Analysis_of_Existing_Bluetooth_Vulnerabilities (Letöltve: 2025. július 10.)
- **ScienceDirect.** (2020) *Security Threats in Brain-Computer Interfaces.* https://www.sciencedirect.com/science/article/pii/S2352914820306407 (Letöltve: 2025. július 19.)
- **ScienceDirect.** (2023) *Secure BCI Architectures for Medical Applications.* https://www.sciencedirect.com/science/article/abs/pii/S1746809423009813 (Letöltve: 2025. július 16.)
- **Springer.** (2024) *BCI Security: Standards and Challenges.* https://link.springer.com/chapter/10.1007/978-981-96-5597-7_19 (Letöltve: 2025. július 12.)
- **Unite.AI.** (2024) *Empathetic AI: Transforming Mental Healthcare and Beyond with Emotional Intelligence.* https://www.unite.ai/empathetic-ai-transforming-mental-healthcare-and-beyond-with-emotional-intelligence/ (Letöltve: 2025. július 7.)
- **Wired.** (2012) *Researchers Hack Brainwaves to Reveal PINs, Other Personal Data.* https://www.wired.com/2012/08/brainwave-hacking (Letöltve: 2025. július 31.)
- **Wired.** (2017) *A New Pacemaker Hack Puts Malware Directly on the Device.* https://www.wired.com/story/pacemaker-hack-malware-black-hat (Letöltve: 2025. július 26.)
- **HIPAA Journal.** (2020) *Serious Vulnerabilities Identified in Medtronic MyCareLink Smart Patient Readers.* https://www.hipaajournal.com/serious-vulnerabilities-identified-in-medtronic-mycarelink-smart-patient-readers (Letöltve: 2025. július 28.)
- **Rostami, Mohammad; Juels, Ari; Koushanfar, Farinaz.** (2013) *Heart-to-Heart (H2H): Authentication for Implanted Medical Devices.* USENIX Security Symposium. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf (Letöltve: 2025. július 21.)
- **Schindler, Philipp; Weichbrodt, Nico; Buhren, Jonas; Kurmus, Ayoub; et al.** (2016) *Intrusion Detection for Implantable Medical Devices: A Runtime Verification Approach.* ETH Zurich. https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/meddev/677.pdf (Letöltve: 2025. július 16.)
- **U.S. Food and Drug Administration (FDA).** (2024) *Biometric Monitoring Technology—Device Summary.* https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=175194 (Letöltve: 2025. július 18.)

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2025