BÁNKI KÖZLEMÉNYEK --- BÁNKI REPORTS
VI. ÉVFOLYAM 2. SZÁM --- VOLUME VI NO. 2

Bevezetés az IoT világába: azon belül testek internete és kiberbiztonság

Introduction to the world of IoT: including the internet of Bodies and cyber security

Nagy Attila*, Horváth-Kiss Anikó**, Rajnai Zoltán***

Óbudai Egyetem, Budapest, Magyarország

*attila.nagy@uni-obuda.hu; **kiss.aniko@bgk.uni-obuda.hu; ***rajnai.zoltan@bgk.uni-obuda.hu

Összefoglalás **— A cikk fő célja a Dolgok Internetének bemutatása, különös tekintettel a Testek Internetére. Célja, hogy ráirányítsa a figyelmet a jövőben rejlő lehetőségekre ezen a területen, miközben felhívja a figyelmet a kiberbiztonsággal kapcsolatos kihívásokra. Az emberi testek internetkapcsolatának előretörése a társadalmak egészségesebbé válásához vezethet, ami miatt kiemelten fontos lesz a megfelelő védelem biztosítása.**

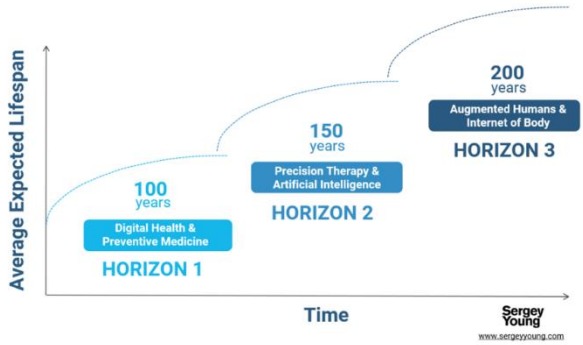
Kulcsszavak**:** IoT, IoB, sérülékenységek

Abstract — The main purpose of this article is to present the Internet of Things, with special regard to the Internet of Bodies. It aims to focus attention on future opportunities in this field while raising awareness of the challenges associated with cyber security. Advances in the Internet connection of human bodies can lead to healthier societies, which makes it extremely important to ensure adequate protection.

Keywords**:** IoT, IoB, vulnerabilities

1 BEVEZETÉS

A longevitás (a hosszú élet tudománya) egy viszonylag új kutatási terület. A longevitás területe forradalmi változásokat hozhat az emberi társadalmakban. Akár 100, 150 vagy 200 évig is élhet majd az ember. Persze ez még egy hosszú folyamat lesz az emberiségnek, de a lehetőségek kezdenek megnyílni. [1] A fejlődési szakaszok három horizontra vannak bontva. Az első horizont a digitális egészségügy és a megelőző gyógyászat technológiai fejlődésére épül, amelyek segítségével átlagosan 100 évig élhetünk. A második horizont a mesterséges intelligenciát (AI) és a precíziós terápiákat foglalja magában, amelyek potenciálisan 150 évre növelik élettartamunkat. A harmadik horizont pedig a kiterjesztett emberek és a testek internete (IoB) innovációinak és fejlesztéseinek köszönhető, amelyek potenciálisan 200 éves (vagy több!) átlagos élettartamot eredményezhetnek. Az (1. ábrán) lehet megnézni a különböző horizontokat. [2]



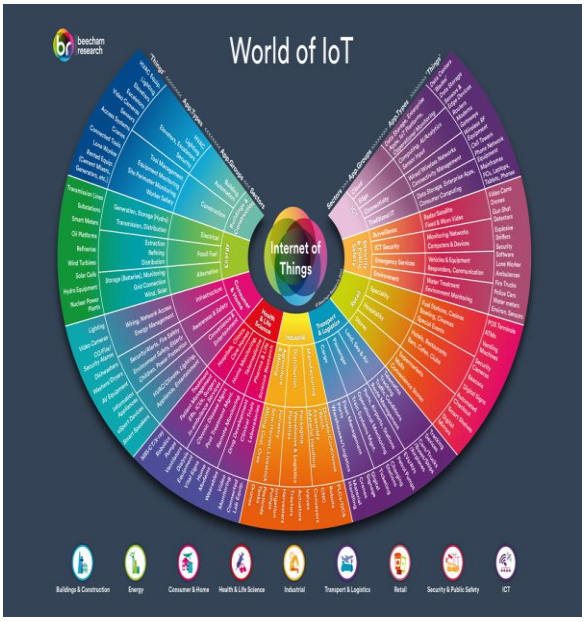
1. ábra: A hosszú élettartam innovációjának horizontja

Az ember életének meghosszabbítása és minőségének javítása több tényezőn múlik. Az egyik ilyen tényező a testek internete (IoB). Ebben a részben először is bemutatjuk a dolgok internetét (IoT), majd áttérünk a testek internetére, ismertetjük a hozzá tartozó eszközöket, végül pedig megvizsgáljuk a potenciális biztonsági kockázatokat. Ha az emberek élettartamának növelésében a Testek Internete kulcsszerepet játszik, akkor a biztonság kiemelt fontosságú lesz ezen a területen. Természetesen a kiberbiztonság minden szektorban létfontosságú.

2 A DOLGOK INTERNETE

Az „Internet of things” fogalmat, ha magyarra szeretnék fordítani akkor az a dolgok internete. Eme logikát követve,

akkor az „Internet of bodies” magyar fordításban a testek internete lesz. Az olvasóknak szeretnénk bemutatni, hogy mi a testek internete, és hogy milyen kiberbiztonsági veszélyek lehetségesek ezen a területen. Mielőtt bele vágnánk szeretnénk a dolgok internete területeit bemutatni, és hogy mi tartozik hozzá nagyvonalakban, a következő ábrán látható az IoT világának területitérképe, melyet 2008-ban vezettek be (2. ábra).



2. ábra: Az IoT területei

Kilenc kulcsfontosságú üzleti területet tartalmazz, melyek a következők: építés és építőipar, energia, fogyasztói és otthoni, egészség és élet tudomány, ipari, szállítás és logisztika, kiskereskedelem, biztonság és közbiztonság, információs és kommunikációs technológia (ICT). [3]

Építés és építőipar: Az IoT alkalmazása az építészetben és építőiparban lehetővé teszi az intelligens épületek és infrastruktúrák létrehozását, amelyek hatékonyabb energiafelhasználást, jobb fenntarthatóságot és magasabb biztonsági szintet biztosítanak. [4]

Energia: Az IoT technológiák segítségével az energiaipar hatékonyabbá válhat, lehetővé téve az okos mérők, energiahatékony rendszerek és a távoli energiakezelés bevezetését, ami csökkentheti az energiafelhasználást és a költségeket. [5]

Fogyasztói és otthoni: Az IoT megoldásokkal a fogyasztók számára intelligens otthonok és okos eszközök nyújtanak kényelmet, energiahatékonyságot és biztonságot, miközben lehetővé teszik az eszközök távoli vezérlését és felügyeletét. [6]

Egészség és élet tudomány: Az IoT az egészségügyben és élet tudomány területén lehetővé teszi az okos egészségügyi eszközök, távmonitorozás és egészségügyi adatelemzés fejlesztését, amelyek segítenek a betegségek korai felismerésében és a betegellátás javításában. [7]

Ipari: Az IoT alkalmazása az ipari területeken lehetővé teszi a gyártási folyamatok automatizálását, az üzemhatékonyság javítását és a gyártási adatok elemzését, ami növeli a termelékenységet és csökkenti a költségeket. [8]

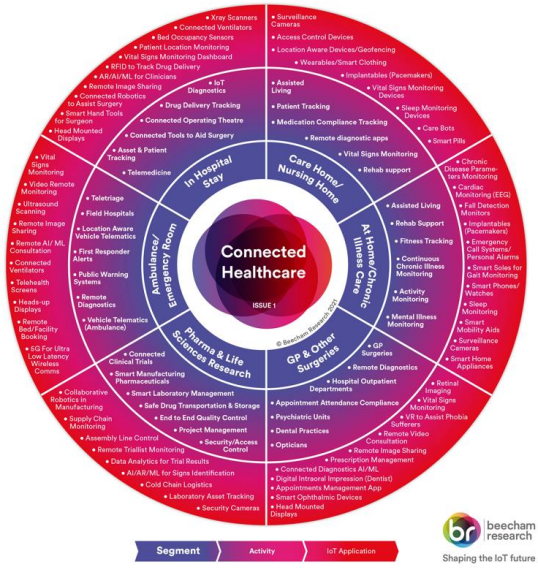
Szállítás és logisztika: Az IoT technológiák alkalmazása a szállításban és logisztikában lehetővé teszi az okos járművek, flottakezelés és raktározás fejlesztését, ami javítja az áruk követését, a szállítási hatékonyságot és a logisztikai folyamatokat. [9]

Kiskereskedelem: Az IoT megoldások alkalmazása a kiskereskedelmi területen lehetővé teszi az okos üzletek, az élmény alapú kiskereskedelem és a vásárlói analitika fejlesztését, ami növeli a vásárlói elköteleződést és javítja az élményt. [10]

Biztonság és közbiztonság: Az IoT technológiák alkalmazása a biztonság és közbiztonság területén lehetővé teszi a térfigyelő rendszerek, okos városok és vészhelyzeti felügyelet fejlesztését, ami javítja a bűn- és balesetmegelőzést, valamint az incidenskezelést. [11]

Információs és kommunikációs technológia (ICT): Az IoT integrálása az információs és kommunikációs technológiák területén lehetővé teszi az okos hálózatok, a távoli elérés és a felhőalapú szolgáltatások kialakítását, ami elősegíti az adatok hatékonyabb kezelését és az információk könnyebb elérését. Ez a fejlesztés lehetővé teszi az üzleti folyamatok automatizálását, az adatelemzési és döntéstámogató rendszerek kialakítását, valamint az ügyfélkapcsolatok és szolgáltatások optimalizálását. Az IoT és az ICT összekapcsolása a digitális átalakulás egyik kulcsfontosságú tényezője, ami új üzleti lehetőségeket teremt és javítja a vállalatok hatékonyságát és versenyképességét. [12]

Az összekapcsolt egészségügyhöz is nagyon sok eszköz tartozik és terület melyet a következő ábrán lehet megnézni (ábra 2.)



3. ábra: A hat kulcsfontosságú területet

Az 3. ábrán hat kulcsfontosságú területet emelnek ki, melyek a következők: kórházi tartózkodás, gondozás otthon és idősek otthona, otthon és krónikus betegség ellátás, háziorvosi rendelők és más műtétek, gyógyszergyártás és élettudományok kutatás, mentők és sürgősségi szoba. [13] A testek internete a krónikus betegség ellátás területéhez tartozik. Ez a terület olyan eszközöket és technológiákat foglal magában, amelyek lehetővé teszik az egészségügyi adatok gyűjtését és elemzését az otthoni környezetben élő emberek számára, például okos eszközökkel és hordozható egészségügyi eszközökkel.

Minden egyes terület megérdemelne egy saját fejezetet, de mi most a testek internetéről fogunk foglalkozni.

3 TESTEK INTERNETE

A "Testek Internete" kifejezést 2016-ban alkották meg, és ez egy viszonylag új területet jelöl. Ezek az eszközök az emberi testet figyelik biometrikus, fiziológiai vagy viselkedési adatok gyűjtése révén. Az információkat vezeték nélküli vagy hibrid hálózatokon keresztül továbbítják más eszközök felé. Ezután egy központi számítógép elemzi és értékeli ki ezeket az adatokat. [14] Az adatok kiértékelése az adatbányászat segítségével történik így állapítható meg az ember egészségi állapota.

3.1 Eszközök

Okos órák és fitneszkarkötők (Smart watches and fitness trackers)

A jelenleg legnépszerűbb és széles körben elterjedt IoB (Testek Internete) eszközök közé tartoznak az okos órák és fitneszkarkötők. Ezek az eszközök mozgás-, szívritmus- (beleértve az eltérések detektálását), alvás- és az újabb készülékekben a véroxigénszint-monitorozásra képes érzékelőket használnak. Emellett széleskörű egészségügyi és fitnesz támogatást nyújtanak, például képesek figyelemmel kísérni az esetleges eleséseket vagy a szokatlan mozgásmintákat, amelyek görcsrohamot jelezhetnek, és ennek megfelelően értesíthetik a családtagokat és a gondozókat. [15]

"Okos" vagy "digitális" pirulák (’Smart’ or ’digital’ pills)

Az úgynevezett okos pirulák olyan gyógyszerformák, amelyek egy lenyelhető érzékelőt kombinálnak a hagyományos gyógyszerhatóanyaggal. Ezek az érzékelők képesek rögzíteni a bevétel időpontját, az adagot és a gyógyszer típusát, továbbá információt szolgáltatnak a páciens aktivitási szintjéről. Jelenleg is használatosak többek között kemoterápia, valamint bipoláris zavar és skizofrénia kezelésére. A jövőbeni fejlesztések lehetővé tehetik, hogy ezek a pirulák nyomon kövessék a belső állapotokat és a gyógyszerekre adott reakciókat, sőt, automatikusan szabályozzák az adagolást a beteg válaszreakciói alapján. [15]

Okos kontaktlencsék (Smart contact lenses)

Ezek a lencsék lehetővé teszik a vér biomarkereinek, például a glükóz, a koleszterin, a nátrium- és káliumionok monitorozását és értékelését egy nem invazív módon, csupán a szemfolyadék felhasználásával. A jövőben a kiterjesztett valóság alkalmazásával készült kontaktlencsék is megjelenhetnek, amelyek további információkat jelenítenek meg a felhasználó látóterében, vagy akár rögzíthetik is azt, amit az emberek látnak. [15]

Agy-gép interfészek (Brain-computer interfaces)

Az agyi implantátumokat már használják arra, hogy a súlyosan bénult emberek képesek legyenek robotkarokat irányítani a saját táplálkozásukhoz, és közvetlenül szöveget generáljanak (90 karakter per perc sebességgel) az agyi jeleik felhasználásával, nem pedig a neuromuszkuláris útvonalakon keresztül. A nem invazív fejfedők is alkalmazhatók a robotkarok egyre összetettebb irányítására, habár itt a technológiai fejlődés lassabb. Ezen technológiák még nem kerültek kereskedelmi forgalomba. [15]

Mesterséges hasnyálmirigyek (Artificial pancreases)

A mesterséges hasnyálmirigy a folyamatos glükózmonitorozást (CGM) és az inzulinpumpát ötvözi, mesterséges intelligenciát alkalmazva az inzulinadagolás automatizálására a CGM által mért adatok alapján. [15]

Szívritmus-szabályozók (Cardiac pacemakers)

Az összekapcsolt szívritmus-szabályozók képesek valós idejű információkat biztosítani a páciens szívritmus-változásairól, és lehetővé teszik a távoli kezelést, mint például a szívritmus-érzékelési vagy szabályozási küszöbök beállítását. Az újonnan fejlesztett szívritmus-szabályozók képesek a testben történő biológiai lebomlásra, amikor már nincs rájuk szükség, és együttműködve más érzékelőkkel hatékonyabban érzékelik az eltéréseket. [15]

Összekapcsolt ruházat (Connected clothing)

A ruházatba beágyazott érzékelőkkel rendelkező ruhadarabok képesek a szívritmus és a mozgás figyelésére. Egyes darabok monitorozzák a testhőmérsékletet is, és képesek alkalmazkodni, hogy a viselőjük kényelmesen érezze magát. Az okospelenkák újítása, hogy képesek érzékelni és jelenteni az újszülöttek bélműködését. [15]

Érzékelőkkel felszerelt kórházi ágyak (Sensor-equipped hospital beds)

Az érzékelőkkel felszerelt kórházi ágyak olyan beépített szenzorokkal rendelkeznek, amelyek képesek a testhőmérséklet, szívverés, véroxigén-szint, vérnyomás és egyéb élettani adatok folyamatos monitorozására. Ez lehetővé teszi az egészségügyi személyzet számára, hogy valós időben nyomon kövessék a betegek alapvető élettani paramétereit. [15]

Figyelő monitorok (Attention monitors)

A szemkövetés olyan technológia, amely meghatározza, hogy egy személy hova néz, legyen szó számítógéphez rögzített eszközről irodai környezetben vagy szemüvegről vezetés közben és mindennapi helyzetekben. Néhány fejlettebb prototípus képes az agyi tevékenység észlelésére és a szemmozgások elemzésére is, így valós időben képesek különböző kognitív folyamatokat, mint a kognitív terhelés, a fáradtság, az elkötelezettség és a figyelem monitorozására. Ezek az eszközök hang- vagy tapintási visszajelzést is adhatnak, például, ha egy felhasználó figyelmetlenné válik. [15]

Testbe ültetett érzékelők (Body-implanted sensors)

A bőr alá ültethető bioszenzorok lehetővé teszik a biológiai folyamatok pontosabb és részletesebb nyomon követését a hagyományos viselhető eszközöknél. Ezek az eszközök továbbfejlesztett funkciókkal is rendelkeznek, mint például egy bőrbe integrált interfész, amely lehetővé teszi a felhasználó számára, hogy távolról irányítsa más eszközöket. További fejlesztés alatt álló érzékelők, amelyeket a fogakhoz rögzítenek, képesek monitorozni a felhasználó által bevitt glükóz, só és alkohol mennyiségét. [15]

Női technológiai termékek (Female technology products)

Egyre több technológiai terméket fejlesztenek ki kifejezetten a nők egészségének és jóllétének elősegítésére; ezeket gyakran "femtech" termékeknek nevezik. A Testek Internete kategóriájába tartozó eszközök között megtalálhatók a hordozható mellszívók, a medencefenék-erősítő eszközök, hűsítő hatású karkötők, amelyek enyhítik a hőhullámokat, valamint olyan csatlakoztatott készülékek, amelyek képesek a méhnyak nyálka monitorozására a termékenység nyomon követése érdekében.

Beültethető mikrochipek (Implantable microchips)

Az RFID és NFC (Near field communication) mikrochipek az emberi testbe ültethetők információk tárolására, mint például a személyes adatok vagy az ajtók nyitására és vásárlások lebonyolítására.

Érzelmi szenzorok (Emotion sensors)

Az érzelmeket érzékelő eszközök, amelyek még fejlesztés alatt állnak, képesek azonosítani a felhasználó érzelmi állapotát az arc kifejezése, mikromozgások, testtartás, gesztusok, agyi és szívtevékenység, bőrvezetőképesség és egyéb jelek alapján. Ezek az adatok felhasználhatók olyan környezeti változtatások elérésére, amelyek javítják a hangulatot.

Látás- és hallássegítő eszközök (Vision and hearing aids)

Számos viselhető eszköz és implantátum áll rendelkezésre, beleértve a beépített kamerával rendelkező mesterséges lencséket és cochleáris eszközöket, amelyeket az érzékelés helyreállítására vagy fokozására használhatnak. Ezek az eszközök lehetővé teszik videó- és hangfelvételek készítését, valamint képesek azonosítani, ha a felhasználó elesett, együtt más viselkedési jelzőkkel.

Wellness-szkennelő alkalmazások (Wellness scanning apps)

Egyes vállalatok olyan technológiákat fejlesztenek, amelyek lehetővé teszik az egészségi állapot mérését invazív beavatkozások és különleges eszközök nélkül. Egy ilyen alkalmazás képes a hagyományos okostelefon-kamerával készített, 30 másodperces arcvideó elemzésével becsülni a pulzusszámot, a stressz szintet és további egészségügyi jellemzőket, majd ezek alapján egy átfogó "wellness" pontszámot adni.

Olfaktorikus érzékelők (Olfactory sensors)

Ezeket az érzékelőket okosfogkefékbe építhetik be vagy önálló modulként alkalmazhatják, hogy gyűjtsék a felhasználó leheletéből származó apró, a biológiai aktivitáshoz vagy betegségekhez kapcsolódó anyagmennyiségeket.

Bőrre felhelyezhető érzékelők („ESkin”) (Sking applied sensors)

Rugalmas fóliaérzékelők, amelyeket tapasz formájában helyezhetünk a bőrre, és amelyek képesek jeleket rögzíteni, mint például a szívverés — ami a fóliát rezgésbe hozza — és az izzadságszint, amelyre a fólia sóval érintkezve reagál.

Hordozható agyi szenzorok (Wearable brain sensors)

Olyan fejhallgatók, amelyek elektromos agyi aktivitást mérnek a fejbőrön elhelyezett elektródák segítségével. Ezáltal képesek például a koncentráció szintjének és a fáradtságnak a megállapítására. [15]

A könnyebb átláthatóság végett egy táblázatba szedtük a különböző IoB eszközöket.

1. táblázat: IoB eszközök

IoB eszközök
Okos órák és fitneszkarkötők
"Okos" vagy "digitális" pirulák
Okos kontaktlencsék
Agy-gép interfészek
Mesterséges hasnyálmirigyek
Szívritmus-szabályozók
Kapcsolt ruházat
Érzékelőkkel felszerelt kórházi ágyak
Figyelő monitorok
Testbe ültetett érzékelők
Női technológiai termékek
Beültethető mikrochipek
Érzelmi szenzorok
Látás- és hallássegítő eszközök
Wellness-szkennelő alkalmazások
Olfaktorikus érzékelők
Bőrre felhelyezhető érzékelők
Hordozható agyi szenzorok

4 SÉRÜLÉKENYSÉGEK

4.1 *OWASP top 10 IoT*

Gyenge, kitalálható vagy beépített jelszavak (Weak guessable, or hardcoded passwords)

Az IoT eszközök gyakran rendelkeznek webalapú felületekkel, amelyeket konfigurációra és kezelésre használnak, ezek mellett hitelesítési mechanizmusok is találhatók az eszközökben, mint például soros konzolok, hálózati szolgáltatások stb. Ha ezeket a felületeket nem megfelelően állítják be, a támadók hozzáférhetnek érzékeny információkhoz és engedély nélkül módosíthatják az eszköz beállításait. A SISA IoT biztonsági tesztelése során kiderült, hogy a tesztelt IoT eszközök többségénél kitalálható jelszavak és felhasználónév lista volt használatban. Egy másik kritikus hiba a rögzített jelszavak beépítése, ahol a fejlesztők beprogramozott hitelesítő adatokat helyeznek az IoT eszközök komponenseibe, például a firmware-be.

A támadás enyhítése:

A gyártóknak megfelelő hitelesítési és jelszókezelési kontrollokat kellene bevezetniük annak biztosítása érdekében, hogy a jelszavak biztonságosak és nehezen kitalálhatóak legyenek. Továbbá a felhasználókat arra kellene ösztönözni, hogy változtassák meg az alapértelmezett jelszavakat az eszközeiken, és az eszközök beállításakor használjanak erős, egyedi és összetett jelszavakat. [16],[17]

Nem biztonságos hálózati szolgáltatások (Insecure network services)

A nem biztonságos hálózati szolgáltatások a hálózati protokollok, szolgáltatások vagy konfigurációk sebezhetőségeire utalnak, és általában magukban foglalják a nem titkosított kommunikációs protokollokat, a gyenge hálózati biztonsági beállításokat, valamint az elavult vagy sebezhető szoftverek használatát. A támadók ezeket a sebezhetőségeket kihasználva lophatnak érzékeny adatokat, indíthatnak támadásokat más rendszerek ellen, vagy jogosulatlanul férhetnek hozzá az eszközhöz.

A támadás enyhítése:

A biztonságos hálózati protokollok, például a Transport Layer Security (TLS) alkalmazása, valamint a hálózati szolgáltatások rendszeres frissítése segíthet enyhíteni ezt a sebezhetőséget. A SISA azt is javasolja, hogy rendszeresen végezzenek hálózati sebezhetőségi értékelést és vörös csapat gyakorlatokat az IoT hálózatokban lévő kritikus biztonsági hibák azonosítása érdekében. [16],[17]

Nem biztonságos ökoszisztéma interfészek (Insecure ecosystem interfaces)

Ez a sebezhetőség az IoT ökoszisztéma különböző komponensei közötti nem biztonságos interfészekből ered. Sok IoT eszköz gyengén védett interfészekkel rendelkezik (web, API, mobil interfészek) külső rendszerekkel, mint például felhőszolgáltatások, más IoT eszközök és hagyományos IT rendszerek. A támadók ezeket az interfészeket használhatják érzékeny adatok elérésére, támadások indítására más rendszerek ellen, vagy az eszköz és annak funkcióinak irányítására. A SISA IoT biztonsági tesztelő csapata egy piacvezető IoT eszköz biztonságának értékelése során találkozott egy olyan API-val, amelynek segítségével minden felhasználó UUID-ját generálhattuk, és felhasználhattuk annak élő helyzetének, jelszavaknak, az alkalmazáshoz csatlakoztatott egyéb eszközeinek, e-mail címének stb. megszerzésére. Annak ellenére, hogy az eszközalkalmazásnak 300 ezer+ letöltése van iOS-en és Androidon, és a gyártónak több mint 100 éves piaci múltja

van, ez a sebezhetőség a hatékony biztonsági intézkedések hiányára utal.

A támadás enyhítése:

Az API-k gyakori frissítése, szigorú hozzáférés-szabályozás alkalmazása a bizalmas API-khoz és interfészekhez való hozzáférés korlátozására, biztonságos kommunikációs csatornák megvalósítása az IoT ökoszisztéma különböző komponensei között, valamint titkosítás alkalmazása ajánlott intézkedések ennek a sebezhetőségnek a mérséklésére. [16],[17]

Biztonságos frissítési mechanizmus hiánya (Lack of secure update mechanism)

Az IoT eszközök gyakran úgy vannak tervezve, hogy alacsony költségűek, kis energiafogyasztásúak és könnyen használhatóak legyenek, ami azt eredményezheti, hogy a biztonsági szempontokat figyelmen kívül hagyják a tervezési folyamat során. Különösen a biztonságos frissítési mechanizmus hiánya teszi az IoT eszközöket sebezhetővé az ismert biztonsági résekkel és kihasználási lehetőségekkel szemben. A támadók kihasználhatják az elavult firmware-t vagy szoftvert az eszköz biztonságának kompromittálására. Az IoT fizetési rendszerekben ez a sebezhetőség komoly következményekkel járhat, beleértve a pénzügyi veszteségeket, a bizalmas információkhoz való jogosulatlan hozzáférését, és a kritikus rendszerek működésének zavarását.

A támadás enyhítése:

Az ilyen funkciók bevezetése, mint a digitális aláírások, a visszaállítás elleni mechanizmusok, a biztonságos szállítás (a frissítés titkosított formában történő küldése, a frissítés aláírása stb.), valamint a firmware hitelesítése az eszközön segíthet a gyártóknak kezelni ezt a sebezhetőséget. [16],[17]

Nem biztonságos vagy elavult komponensek használata (Use of insecure or outdated components)

Az IoT eszközökben használt nem biztonságos vagy elavult komponensek alkalmazása egyre növekvő aggodalomra ad okot a technológia világában. Sok IoT eszköz harmadik féltől származó komponensek felhasználásával készül, amelyek tartalmazhatnak sebezhetőségeket, amiket a támadók kihasználhatnak az eszköz biztonságának kompromittálására.

A támadás enyhítése:

Az IoT eszközökben használt összes szoftver és komponens (beleértve a firmware-t, könyvtárakat és keretrendszereket) rendszeres frissítése és javítása, valamint egy folyamat létrehozása a komponensekben lévő biztonsági sebezhetőségekről szóló értesítések figyelemmel kísérésére és fogadására az IoT ökoszisztémában, a sebezhetőség mérséklésének néhány legjobb gyakorlata. [16],[17]

Elégtelen adatvédelem (Insufficient privacy protection)

Sok IoT eszköz gyűjt és tárol érzékeny személyes adatokat, azonban gyakran hiányoznak a megfelelő adatvédelmi és adatbiztonsági intézkedések. Ez magában foglalhatja az adatgyűjtést a felhasználó beleegyezése nélkül, az adatok biztonsági ellenőrzések nélküli tárolását, valamint az adatok megfelelő engedélyek nélküli harmadik felekkel történő megosztását.

A támadás enyhítése:

Az adatvédelmi elvek tervezésbe történő beépítése, a titkosítás alkalmazása az érzékeny adatok továbbítása és tárolása során, valamint a felhasználók beleegyezésének megszerzése az adatgyűjtéshez és felhasználáshoz azok az effektív mérséklő intézkedések, amelyek alkalmazhatók. [16],[17]

Nem biztonságos adatátvitel és tárolás (Insecure data transfer and storage)

Az IoT eszközök esetében komoly aggodalomra ad okot az adatok titkosítás nélküli, nyílt szöveges átvitele és tárolása. Az IoT eszközök nagy mennyiségű személyes és érzékeny információt gyűjtenek és tárolnak, és a támadók közbeékelődhetnek az adatátvitelbe vagy manipulálhatják az adatokat azok továbbítása során, illetve kihasználhatják a gyenge tárolási mechanizmusokat.

A támadás enyhítése:

Biztonságos protokollok, mint például az HTTPS használata az adatátvitelhez, az érzékeny adatok nyugalmi állapotban történő titkosítása, szilárd hozzáférés-szabályozási rendszerek kialakítása, valamint az adattárolási gyakorlatok rendszeres auditálása hatékony intézkedések az IoT eszközök adatátvitelének és tárolásának biztosítására. [16],[17]

Eszközkezelés hiánya (Lack of device management)

Az IoT eszközök hatékony kezelésének hiánya veszélyeztetheti az egész hálózatot. Az effektív eszközkezelés hiánya lehetővé teszi a támadók számára, hogy távolról manipulálják vagy irányítsák az IoT eszközöket. A nem megfelelő kezelés jogosulatlan hozzáférést, firmware manipulációt vagy az eszközök módosítását eredményezheti. A SISA IoT eszköztesztelési értékelései során több esetben is kiderült, hogy az eszközök lejárt SSL tanúsítványokkal rendelkeztek, így a webes kommunikáció HTTP-n keresztül történt. Mivel az eszköz nem biztosított frissítéseket, az SSL tanúsítványok nem lettek megújítva, ami sebezhetővé tette az eszközt.

A támadás enyhítése:

Erős hitelesítési mechanizmusok, mint például egyedi eszközhitelesítő adatok bevezetése, és a hozzáférés-szabályozások érvényesítése, hogy az eszközkezelési funkciók csak a jogosult személyzet számára legyenek elérhetőek, csökkentheti ezt a kockázatot. [16],[17]

Nem biztonságos alapértelmezett beállítások (Insecure default settings)

Az IoT eszközökön azok a konfigurációk, amelyeket a gyártó változatlanul hagy, potenciális biztonsági kockázatoknak tehetik ki az eszközt. Ezek a beállítások magukban foglalhatják az alapértelmezett felhasználóneveket és jelszavakat, nyitott portokat és a nem titkosított kommunikációt. Gyakran az alapértelmezett beállítások a "minimális" megközelítést képviselik, vagy akár bevezethetnek IoT biztonsági sebezhetőségeket, például beépített jelszavakat vagy root jogosultságokkal futó kitett szolgáltatásokat.

A támadás enyhítése:

Az alapértelmezett felhasználónevek, jelszavak és konfigurációk megváltoztatása az eszközök első beállítása során, valamint a szükségtelen szolgáltatások és portok letiltása a támadási felület csökkentése érdekében olyan intézkedések, amelyek mérsékelhetik ezt a sebezhetőséget. [16],[17]

Fizikai védelem hiánya az IoT rendszerekben (Lack of physical hardening)

Az IoT rendszerek fizikai védelem hiányára utal, ha nem valósítanak meg fizikai biztonsági intézkedéseket. Ez teszi a beágyazott eszközöket sebezhetővé különféle hardveres támadásokkal és firmware manipulációval szemben, így engedélyezve a hackerek számára az olyan jogosulatlan hozzáféréseket, mint a root soros bejelentkezés, érzékeny információk kinyerése stb., amelyek távoli támadások végrehajtására vagy az eszköz feletti irányítás megszerzésére használhatók.

A támadás enyhítése:

Néhány intézkedés, amelyet meg lehet tenni az eszköz fizikai megerősítésére, beleértve a hibakereső portok letiltását vagy elszigetelését, a biztonságos indítás használatát a firmware érvényesítésére, a manipuláció-észlelési mechanizmusok alkalmazását, valamint az érzékeny információk eltávolítható memóriakártyán való tárolásának elkerülését. [16],[17]

5 ÖSSZEGZÉS

A kutatási terület, amit "longevitás" néven ismerünk, a hosszú élet tudománya, és viszonylag újnak számít. Ez a tudományág jelentős változásokat hozhat az emberi társadalmakban, például elősegítheti, hogy az emberek akár 100, 150, vagy akár 200 éves korukig is éljenek. Ez egy hosszú folyamat lesz az emberiség számára, de a lehetőségek már kezdenek körvonalazódni. A longevitás fejlesztési szakaszait három "horizont" jellemzi: az első a digitális egészségügy és a megelőző gyógyászat technológiai fejlődésére épül, a második horizont a mesterséges intelligenciát (AI) és a precíziós terápiákat foglalja magában, míg a harmadik a kiterjesztett emberek és a testek internete (IoB) innovációira támaszkodik. Ezek a fejlesztések potenciálisan lehetővé teszik az emberek számára, hogy jelentősen meghosszabbított életet éljenek.

A "testek internete" (IoB) olyan technológiát jelent, amely az emberi testen viselhető vagy beültetett eszközökkel gyűjt adatokat, mint például biometrikus, fiziológiai vagy viselkedési információkat. Ezek az adatok vezeték nélküli vagy hibrid hálózatokon keresztül továbbíthatók más eszközökre, ahol központi számítógépek elemezhetik és értékelhetik ki őket. Az IoB eszközök jelentőségét nem csak a hosszabb élettartam elősegítésében, hanem a mindennapi egészségügyi és életminőségi javulásokban is kiemelkedőnek ígérkezik.

A "dolgok internete" (IoT) szintén fontos szerepet játszik, különböző üzleti területeken belül, mint például az építőipar, az energiaipar, a fogyasztói és otthoni eszközök, az egészségügy és élettudományok, az ipar, a szállítás és logisztika, a kiskereskedelem, a biztonság és közbiztonság, valamint az információs és kommunikációs technológiák. Ezek a területek hozzájárulnak az okos infrastruktúrák létrehozásához, az energiafelhasználás hatékonyságának javításához, az intelligens egészségügyi eszközök fejlesztéséhez, és számos más előnnyel szolgálnak mind a magánszemélyek, mind a társadalom számára.

A longevitás és az IoB további kutatása és fejlesztése kulcsfontosságú lesz az emberiség jövője szempontjából, hiszen ezek a technológiák nem csupán az élet hosszát képesek növelni, hanem a minőségét is jelentősen javítani. Azonban fontos, hogy ezen technológiák fejlődése mellett a kiberbiztonsági kihívásokra is nagy figyelmet fordítsunk, hiszen az adatvédelem és a biztonságos használat garantálása nélkülözhetetlen a felhasználók bizalmának megőrzéséhez.

IRODALOMJEGYZÉK

[1] S. Young, *A fiatalodás tudománya*. 2023.
[2] S. Young, "Three Horizons of Longevity Innovation." [Online]. Available: https://sergeyyoung.com/three-horizons-of-longevity-innovation, 2020
[3] "World of IoT sector map." [Online]. Available: https://www.beechamresearch.com/download-details/world-of-iot-sector-map/, 2024
[4] "IoT in construction: Top benefits, Use-case and application." [Online]. Available: https://toolsense.io/equipment-management/iot-in-construction-top-benefits-use-cases-application/#:~:text=IoT%20has%20diverse%20applications%20in,on%20time%20and%20within%20budget.
[5] M. M. Alenazi, "IoT and Energy," in *Internet of Things - New Insights*, M. K. Habib, Ed., IntechOpen, 2024. doi: 10.5772/intechopen.113173.
[6] "Everything you need to know about consumer IoT (CIoT)." [Online]. Available: https://www.hitechnectar.com/blogs/consumer-iot-ciot/, 2023
[7] "How Internet of things (IoT) is impacting life sciences and healthcare industry." [Online]. Available: https://www.42gears.com/white-papers/how-internet-of-things-is-impacting-life-sciences-healthcare-industry/, 2023
[8] "What is industrial IoT (IIoT)?" [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-industrial-iot.html
[9] "IoT in transportation and logistics - The ultimate guide." [Online]. Available: https://www.teletracnavman.com/fleet-management-software/telematics/resources/iot-in-transportation-logistics-the-ultimate-guide, 2024
[10] "How IoT in retail is changing the global retail industry." [Online]. Available: https://onomondo.com/blog/how-iot-in-retail-is-changing-the-global-retail-industry/, 2023
[11] "Understanding the IoT for public safety." [Online]. Available: https://iothink-solutions.com/all_resources/understanding-the-iot-for-public-safety/, 2023
[12] "Information and communication technology (ICT)." [Online]. Available: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict, 2023
[13] "Connected healthcare sector chart." [Online]. Available: https://www.beechamresearch.com/download-details/connected-healthcare-sector-chart/, 2024
[14] "What is the Internet of Bodies (IoB), and why should you care?" [Online]. Available: https://itrexgroup.com/blog/internet-of-bodies-iob-definition-benefits-examples/, 2022
[15] "The future of the Internet of Bodies," 2023. [Online]. Available: https://files.microcms-assets.io/assets/8ba880c1ada24b3286662c41b2822851/b70814cee4424407819ae201cca24153/Future%20of%20IoB%20Full%20report%20FINAL%20SOIF%2005.31.pdf, 2023
[16] "Internet of things (IoT) Top 10 2018." [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
[17] "The OWASP IoT top 10 vulnerabilities and how to mitigate them." [Online]. Available: https://www.sisainfosec.com/blogs/the-owasp-iot-top-10-vulnerabilities-and-how-to-mitigate-them/, 2023