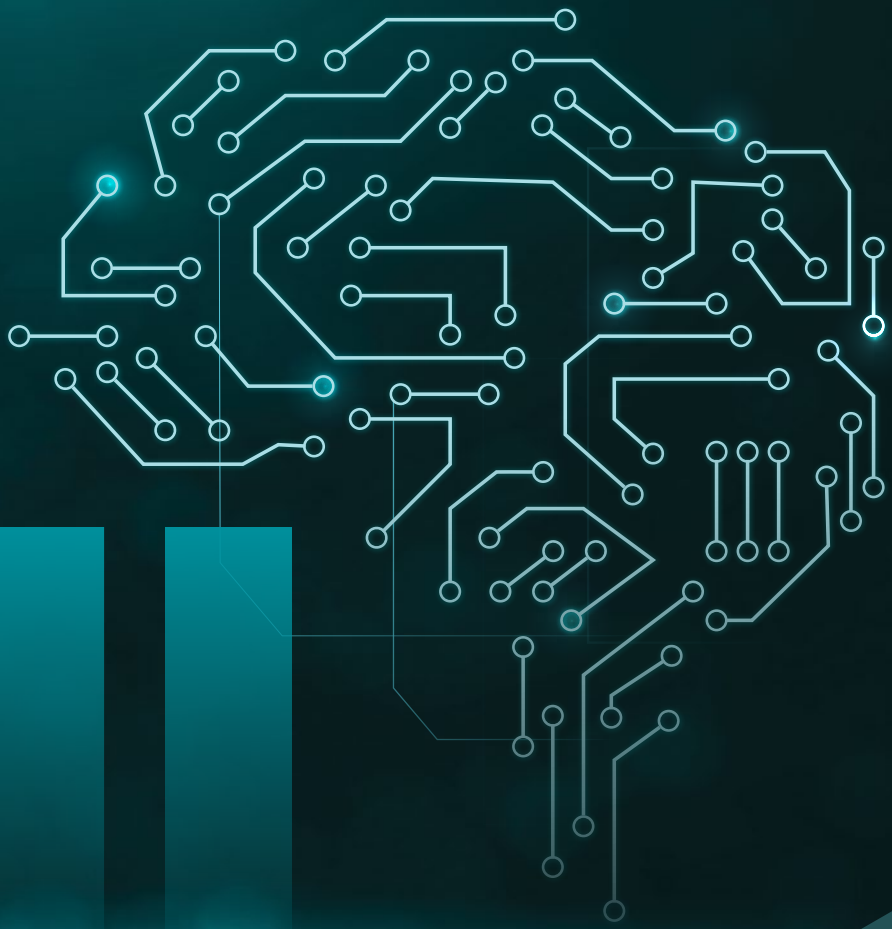


MI A BAJ?

Mesterséges intelligencia, IT-biztonság és mentális egészség

TARTALOM

Mesterséges intelligencia, IT-biztonság és mentális egészség

Ha egy szóban kellene összefoglalni a kort, amelyben élünk, talán a bizonytalanság lenne ez a szó. Az emberiség által ismert, évtizedes, akár évszázados keretek szűnnek meg, miközben olyan technológiákat kezdünk használni, amelyek nyaktörő sebességgel fejlődnek. Eközben nekünk, embereknek a biológia és pár ezer év evolúció eszközkészletével kell feldolgoznunk olyan ugrásokat, amelyek fényévekkel visznek előrébb.

Ilyen a mesterséges intelligencia is, ami fogalomként ugyan évszázadok, akadémikusok által vizsgált területként pedig több évtizede létezik, a gyakorlatban csupán az elmúlt, nagyjából egy emberöltő során vált kézzelfogható valósággá. Tömeges használatáról pedig csak néhány éve beszélhetünk, azonban már ez a rövid idő is elég volt ahhoz, hogy az AI-technológia életünk szinte minden területén megjelenjen valamilyen formában. Nagyobb hatása van, mint az emberiséget szintén alaposan átformáló közösségi médiának, de talán magánál az internetnél is mélyebben nyúl bele és alakítja át a szokásainkat és az egész modern világot.

Akárcsak az internet, a mesterséges intelligencia is kétélű kard az emberiség kezében. Megfelelően használva számtalan új lehetőséget ad a kezünkbe, új alapokra helyezve szinte az egész életünket. Rossz kezekben azonban káoszt és zavart kelt, illetve a megtévesztés, dezinformáció soha nem látott mélységeivel fenyeget.

Az ESET hivatalos forgalmazójaként utóbbival pontosan tisztában vagyunk, hiszen az IT-biztonsági szektor kialakulása óta igyekszik megoldást találni az újabb és újabb fenyegetésekre, vagy megelőzni azokat. A mesterséges intelligencia megjelenésével ez a küzdelem még kiélezettebbé vált.

„Nagyobb hatása van, mint az emberiséget szintén alaposan átformáló közösségi médiának, de talán magánál az internetnél is mélyebben nyúl bele és alakítja át a szokásainkat és az egész modern világot.”

SZOKODI JUDIT

KÖSZÖNTŐ

Éppen ezért éreztük fontos feladatunknak, hogy egyfajta kordokumentumként felmérjük és rögzítsük az AI-jal kapcsolatos hozzáállást a magyar társadalomban, 2026 elején. Az általános használat mellett, különösen kíváncsiak voltunk rá, hogy az IT-biztonság területén milyen hatásokkal, kockázatokkal és fenyegetésekkel kell számolnunk, így ez is a kutatás fontos része lett. Emellett igyekeztünk olyan megközelítést találni, amelyre hazánkban még nem volt példa.

A kor, amelyben élünk, tálcán kínálta a megoldást: napjainkban elég csak körülnézni az online médiumok, közösségi oldalak felületein, ahol egyik AI-generált tartalom követi a másikat. Ezek között akad megmosolyogtatóan művi alkotás, de olyan is, amelyet a szakemberek is csak nehezen tudnak megkülönböztetni a valóságtól.

Ez elgondolkodtató jelenség, fontos kérdés ugyanis, hogy mi történik az emberiséggel, ha elveszítjük a valósággal kapcsolatos egyik legfontosabb "biztonsági réteget". Ha már egyáltalán nem hihetünk az érzékszerveinknek, ha kételkednünk kell az írott tartalmakon túl, az álló és mozgóképek valódiságában is, milyen hatással lesz ez a kollektív pszichénkre? Éppen ezért, a kutatásunk során az AI-használat IT-biztonsági hatásai mellett annak mentális hatásait is igyekeztünk feltérképezni.

Bízom benne, hogy a kutatásunk segítségével rávilágíthatunk a mesterséges intelligencia felelős használatának fontosságára és tényekkel, adatokkal, illetve értékes szakértői gondolatokkal járulhatunk hozzá az erről szóló társadalmi párbeszédhez.

Szokodi Judit
Cégvezető
Sicontact Kft – Az ESET magyarországi hivatalos forgalmazója

„Az AI nem csodafegyver, amely önmagában, emberi beavatkozás nélkül képes lenne minden problémát, feladatot megoldani, hanem egy hatékony segítség ebben. A használata pedig nem előny, hanem az kerül komoly hátrányba, aki nem ismeri, nem használja ezt a technológiát."

A whitepaperhez készült kutatás értelmezésére, feldolgozására több terület ismert, megbecsült szakértőit kértük fel, hogy szakmai tudásukkal járuljanak hozzá a téma alaposabb megértéséhez és az IT-biztonsági, illetve mentális egészségi szempontból fontos összefüggések feltérképezéséhez.

„Azt hiszem, a legnagyobb hibát akkor követjük el, ha az AI használata során nem vesszük észre a kognitív és érzelmi képességeink visszaszorulását és átlagemberként pozitív érzelmi kapcsolatot építünk az algoritmussal, ahelyett, hogy, megtartva a kritikai gondolkodást, eszközként kezelnénk."

Csizmazia-Darab István

Az ESET termékeit forgalmazó Sicontact állandó **IT-biztonsági szakértője,** 1989-ben kezdett számítógép-programozóként dolgozni. A 2000-es évek óta már kizárólag számítógépes biztonsággal foglalkozik, az Antivírus blog szerkesztője és a Hackfelmetszők podcast sorozat szereplője.

„Számomra az AI egyszerre jelent soha nem látott hatékonyságú technológiát, lenyűgöző emergens képességeket, ugyanakkor, kiberbiztonsági stratégaként hatalmas kockázatokat. Ezzel a technológiával meg kell tanulnunk egymás mellett élni, sőt támaszkodni egymás képességeire, ezért meg kell találnunk a megfelelő egyensúlyokat és megfelelően fel kell készülni az AI-eszközök használatára. Tiltás helyett a megismerésben és a technológia megértésében látom a helyzet kulcsát valamint abban, hogy sürgősen meg kell határoznunk az AI megoldások státuszát. Az AI több mint eszköz, de más mint az ember."

Keleti Arthur

Kibertitok jövőkutató, az Informatikai Biztonság Napja (ITBN) konferenciák alapítója és főszervezője, IT-biztonsági és AI stratéga, író, producer.

Tari Annamária

Klinikai szakpszichológus, pszichoterapeuta, pszichoanalitikus. Több éve rendszeresen foglalkozik a fogyasztói társadalom hatásaival, a média és az emberi tényezők összefüggéseivel, a társadalmi változások egyénekre ható vonásaival. Az információtechnológia fejlődésével együtt járó lélektani jellemzők, generációs különbségek és az online élet személyiségre ható változásai a fő kutatási területe.

„A mesterséges intelligencia olyasmi, amit ma már nem tudunk különválasztani a valóságtól. Olyan paradigmaváltásról van szó, ami forradalmasítja a mindennapjainkat, ezért fontos, hogy ne kizárjuk az életünkből, hanem fejlődjünk a változással."

Kerek István

AI-üzletfejlesztési szakértő, az EVERENGINE Kft. cégvezetője és tulajdonosa, egyetemi óraadó tanár, író, a "ChatGPT magyarul" Facebook-csoport alapítója. Három évtizedes IT szakértői szakmai tapasztalattal rendelkezik, a mesterséges intelligenciával 2008 óta foglalkozik. Gyakorlatias szemléletét felhasználva igyekszik megosztani a tudását a területtel kapcsolatban.

BEVEZETŐ

2022. november 30-án új fejezet kezdődött az emberiség életében. Ekkor vált nyilvánosan elérhetővé a ChatGPT, amely bő két hónap alatt, 2023. januárjára már elérte a havi százmillió aktív felhasználót. Ezzel a generatív mesterséges intelligencia (MI/AI)* technológiai újdonságból hétköznapi eszközzé lépett elő. Egyre többen, egyre többféle módon használják, miközben maga a technológia is látványosan fejlődik, gyakran olyan ugrásokkal, amiket követni is nehéz, feldolgozni és értelmezni pedig gyakran még nagyobb kihívást jelent.

MINDEZT JÓL PÉLDÁZZA a Microsoft által 2026. február 10-én közzétett Global Online Safety Survey kutatás, amely 15 országban, közel 15 000 ember megkérdezésével próbálta felmérni, hogy mennyire tudják az emberek megkülönböztetni a valós videókat a deepfake-hamisítványoktól. Az eredmény önmagáért beszél: míg egy évvel korábban még a megkérdezettek 46%-a ismerte fel a deepfake videókat, 2026-ban ez az arány már csak 25% volt, a technológia fejlődése miatt.

Az egyre minőségibb generált tartalmakon túl, ennek a folyamatnak van egy egyelőre csak részben feltárt oldala is, amely túlmutat a hatékonyságon és a produktivitáson. Ha az emberek egyre kevésbé tudják biztosan eldönteni, hogy amit olvasnak, látnak vagy hallanak, az valódi, ez olyan fajta bizonytalanságot eredményezhet a valóságérzékelésünkkel kapcsolatban, ami sokaknál szorongást, stresszt, de akár a kontrollvesztés érzését is kiválthatja. Ha ez megtörténik, az életünk számos területét befolyásolhatja, hiszen elég csak belegondolni, hogy a mindennapi információ-fogyasztásunk alapja a bizalom. Ha ez meginog, az nem csak mentális terhet jelent, mivel fontos döntésekre lehet hatással.

A továbbiakban egy, az ESET számára készült kutatáson keresztül járjuk körül és elemezzük ezt a jelenséget, azaz a generált tartalmak valósághűvé válásából fakadó megkülönböztetési bizonytalanságot és annak lehetséges mentális következményeit. A hazai közbeszédben és az AI-használatról szóló kutatásokban ez a nézőpont jellemzően ritkábban jelenik meg, pedig a következményei több területet is befolyásolnak.

*A mesterséges intelligenciát magyar nyelven gyakran MI-ként említik, az angol artificial intelligence kifejezésből képzett AI rövidítéssel szemben. Ezen kiadvány oldalain azonban maradtunk az AI rövidítésnél, a könnyebb érthetőség és a félreértések elkerülése miatt.

BEVEZETŐ

Az egyik ilyen, kiemelten fontos terület az IT-biztonságé. A modern megtévesztési kísérletek, legyen szó egy főnöktől érkező e-mailről, egy felettest imitáló telefonhívásról vagy bármilyen hitelesnek tűnő üzenetről, arra építenek, hogy a címzett megbízik a tartalomban és gyorsan reagál rá. Ha a tartalom hitelességének megítélése egyre nehezebb, a védekezés sem támaszkodhat a megérzésekre: a bizalom kérdése stratégiai és szervezeti üggyé válik.

Ez a kiadvány ezért három nézőpontból vizsgálja a helyzetet. Bemutatja, hogyan használják ma az emberek az AI-eszközöket a mindennapokban és a munkában; értelmezi az AI-használat IT-biztonsági kockázatait és a szervezeti felkészülés dilemmáit; valamint vizsgálja az AI-hoz kapcsolódó mentális hatásokat, különös tekintettel arra, hogy a valósághű generált tartalmak terjedése hogyan befolyásolhatja a biztonságérzetünket, a valóság feletti kontroll élményét és az ebből fakadó stressz szintjét.

Nem célunk, hogy pánikot keltsünk, és nem is aggatnánk „jó" vagy „rossz" címkéket a technológiai fejlődésre és a mesterséges intelligencia eszközökre. A cél az, hogy a kutatási adatok alapján közérthetően megmutassuk, milyen mintázatok rajzolódnak ki ma, hol vannak a legnagyobb kockázati csomópontok, és felhívjuk a figyelmet arra, hogy a mesterséges intelligencia - illetve tágabban értelmezve az újonnan megjelenő technológiák - a bizalom, a biztonság és a mentális terhelés kérdéseivel összefüggéseiben érdemes foglalkozni.

SZAKÉRTŐI KOMMENTÁR

KELETI ARTHUR

A valóság és az igazság kérdését a filozófia legnagyobb alakjai kutatják évezredek óta. Utóbbi a tények egyfajta interpretációja, amelyekről úgy véljük, megállapítható róluk, hogy valóságosak-e vagy sem.
Az informatika rendszereket pedig éppen azért hoztuk létre, hogy tényeket, adatokat tároljunk bennük, amelyekkel dolgozhatunk és amelyekből még több adatot állíthatunk elő.

Ezért az az érzés alakulhatott ki bennünk, hogy amik az informatikai rendszerekben szerepelnek, azok tények. Sőt, általános megfigyelés szerint bizonyos digitális formátumok használata (mint például a táblázatok) tovább növeli a tényszerűség érzését, különösen a szervezetekben dolgozó emberek között.

Itt lép be a képbe a bizalom kérdése, amit úgy határozhatunk meg, mint a megbízó fél hajlandóságát arra, hogy a megbízottal szemben kiszolgáltatottá tegye magát, mivel feltételezi, hogy utóbbi úgy fog cselekedni, hogy a megbízó érdekeit szolgálja. Azonban, a technológia beágyazódásával a bizalom bináris jellege és általános mivolta megszűnik, a helyét a kontextustól függő, dinamikusan változó bizalom veszi át, amelyet a technológia néhol megerősít, néhol pedig elbizonytalanít.

AI-alapok I.:

Gyors terjedés, lassú szervezeti reakciók

A generatív mesterséges intelligencia terjedését ma két, egyszerre igaz állítás írja le a legpontosabban: sokan már használják, ugyanakkor a munkahelyi keretek sokszor még nem tartanak ott, hogy ezt a használatot tudatosan támogassák vagy biztonságos mederben tartsák.

A

TECHNOLÓGIA JELLEMZŐEN „ALULRÓL" TERJED: először egy-egy ember, munkavállaló, véleményformáló kezdi el kipróbálni és beépíteni a mindennapokba. A szervezeti szintű AI-használattal kapcsolatos döntés, szabályozás, illetve oktatás később jelenik meg.

Az ESET számára elvégzett reprezentatív kutatásból látszik, hogy a mesterséges intelligencia ma már széles körben elért a magyar felhasználókhoz is: a válaszadók közel kétharmada jelezte, hogy használt már valamilyen formában mesterséges intelligencia eszközt.

Ugyanakkor, munkahelyi környezetben a kép jóval kevésbé egyértelmű. A munkahelyi AI-használat nem feltétlenül vezetett folyamatként jelenik meg, hanem gyakran egyéni kezdeményezések mentén, részben láthatatlanul. Ez azért fontos, mert a szervezetek szempontjából a legnagyobb kockázat nem feltétlenül maga az eszköz, hanem ha a használat úgy válik rutinná, hogy közben nincs világos célja, nincs közös értelmezési kerete, és nincs kijelölve, mi az, ami megengedett vagy kockázatos.

SZAKÉRTŐI KOMMENTÁR — **KEREK ISTVÁN**

2025 nyarán végeztem egy „emberkísérletet": AI-jal létrehoztam egy videót, amelyen látszólag egy éjjellátó kamera felvétele látható. A rövid videónak egy medve volt a főszereplője, amely egy családi ház kertjében felállított trambulinon ugrált. A videót néhány nap alatt közel 80 millióan nézték meg és az emberek többsége valósnak gondolta.

Annak ellenére, hogy direkt elhelyeztem a videóban olyan árulkodó jeleket, amelyekből ki lehetett találni, hogy AI-videóról van szó. Ezen azonban az emberek 90%-a átsiklott.
Ezzel próbáltam felhívni a figyelmet arra, hogy ma már mindenkinek sokkal jobban oda kell figyelnie az online tartalmakra, mert egyszerűen nem lesz rá más módszerünk, hogy kiszűrjük a csalásokat.

A kritikus gondolkodást kell előtérbe helyezni, anélkül hatalmas problémánk lesz, mert még a kifejezetten erre fejlesztett AI-detektáló programok sem képesek egyértelműen különbséget tenni a valós és a generált tartalmak között.

> „Kiengedtük a szellemet a palackból, ezzel már együtt kell élnünk, az aggódásra szánt időt pedig oktatásra kell fordítani.”
>
> Szakértő ESET partner

A munkahelyi AI-érettség egyik legjobb indikátora, hogy egy szervezet beszél-e egyáltalán az AI-ról, és ha igen, milyen minőségben. A kutatás szerint sok munkahelyen a téma még nem jelent meg hivatalosan: a dolgozók többsége nem találkozott szervezeti szintű kommunikációval arról, hogy a munkáltató hogyan viszonyul az AI-eszközökhöz. Ahol viszont már felmerült a bevezetés vagy a használat lehetősége, ott is gyakran hiányos a kép. Nem mindig világosak a célok, illetve képzés, tájékoztatás sem feltétlenül társul a bevezetéshez. Ez alapján olyan helyzetkép rajzolódik ki, ahol a technológia gyors munkahelyi megjelenését a közös szabályok és rutinok kialakítása egyáltalán nem, vagy nem kellő gyorsasággal követi le.

Ez a késlekedés sokszor érthető, mivel a technológiai innováció egyik jellemzője, hogy a szabályozás (legyen szó állami, vagy, mint esetünkben, munkahelyi szabályozásról) nem tud lépést tartani az újdonságok bevezetésével. A halogatás viszont komoly kockázatokat rejt, miközben a szervezeti változásmenedzsment, a belső irányelvek kialakítása és a képzés megszervezése időigényes, sokszereplős folyamat. Ezzel szemben egy új eszköz kipróbálása és mindennapi használata percek kérdése. A két sebesség közötti nagyságrendi különbség szinte törvényszerűen létrehoz egy átmeneti állapotot, amikor az adott technológiát már használják, de még nem beszélnek róla. Az ilyen helyzetekben pedig jelentősen megnő a félreértések, a túlzott bizalom, az adatkezelési bizonytalanság vagy a nem kívánt kockázatvállalás esélye.

A következőkben ezért röviden felvázoljuk azt a technológiai hátteret, amely magyarázza, miért vált a generatív AI ilyen rövid idő alatt ennyire meggyőzővé. Ez nem pusztán technikatörténeti kitérő, a fejlődés üteme ugyanis közvetlenül kapcsolódik ahhoz a kérdéshez, amely a kutatás egyik legfontosabb sajátossága is. Minél valósághűbbek a generált tartalmak, annál gyakrabban merül fel a bizonytalanság, hogy amit látunk, hallunk vagy olvasunk, az hiteles-e. Ez a bizonytalanság pedig egyszerre válhat mentális teherforrássá és IT-biztonsági kockázati tényezővé.

AI-alapok II.:

Általános technológiai háttér

A generatív mesterséges intelligencia (genAI) fejlődését nem pusztán az jelzi, hogy egyre több feladatra használjuk, hanem az is, hogy a kimenetek egyre inkább alkalmasak rá, hogy valóságélményt keltsenek. Ma már nemcsak arról van szó, hogy egy eszköz gyorsan összeállít egy vázlatot vagy összefoglalót, hanem arról is, hogy a szöveg, a kép, a videó vagy a hang gyakran annyira meggyőző, hogy a befogadó számára nehézzé válik a hitelesség megítélése.

NAGY NYELVI MODELLEK (LLM-EK) FEJLŐDÉSE JÓ PÉLDA ERRE. A korai, széles körben elérhető generatív megoldásoknál a pontatlanság és a következetlenség könnyebben tetten érhető volt. Gyakori volt, hogy „darabos" volt a szöveg, félrecsúszott a feladatértelmezés, a felhasználónak pedig több korrekcióra volt szüksége. A mai genAI-eszközök ezzel szemben sokkal természetesebb párbeszédre képesek, ami a felhasználói élmény szintjén egyre inkább olyan érzéseket kelt, mintha egy kompetens asszisztenssel beszélgetnénk. Ezt a minőségi ugrást a kutatásban az is visszajelzi, hogy az AI-t használók döntő többsége elégedett a kapott eredményekkel.

A technológiai fejlődés hátterében az AI-eszközök úgynevezett "kontextushosszának" (context length) ugrásszerű növekedése áll. Ez mutatja meg, hogy egy generatív nagy nyelvi modell (mint a ChatGPT, Gemini, stb.) mennyi információt képes értelmezni egy utasítás, azaz prompt esetén. Ezt a hosszt úgynevezett tokenekben mérik, leegyszerűsítve egy token nagyjából egy szónak felel meg. A ChatGPT 2022-es indulásakor az akkori felhasználóknak egy 2000 tokenből álló kontextusba kellett csomagolnia az LLM-nek szánt utasításaikat. Ez körülbelül 8 oldal szöveget jelent (szimpla sorköz, 12-es betűméret esetén). Már ez is meglehetősen alapos leírásra ad lehetőséget, azonban érdemes szembeállítani mindezt azzal, hogy bizonyos felhasználási keretek között (API-n keresztül) bizonyos modellek ma már a 2-4 millió tokenből álló kontextust is képesek kezelni. Összehasonlításként, ez annyit jelent, hogy ma már egy-egy promptba könnyedén beleférne A Gyűrűk Ura-trilógia kétszer (!) és egy teljes, angol nyelvű King James Biblia. Ez pedig csak a kezelhető utasításkészlet méretét jelzi, ami talán rávilágít, hogy mekkora technológiai ugráson vagyunk túl a nagy nyelvi modellek esetén.

Hasonló fejlődés figyelhető meg a képgenerálásban, illetve az AI által létrehozott videóknál is. Korábban a generált képeknél és videóknál gyakoriak voltak az árul-

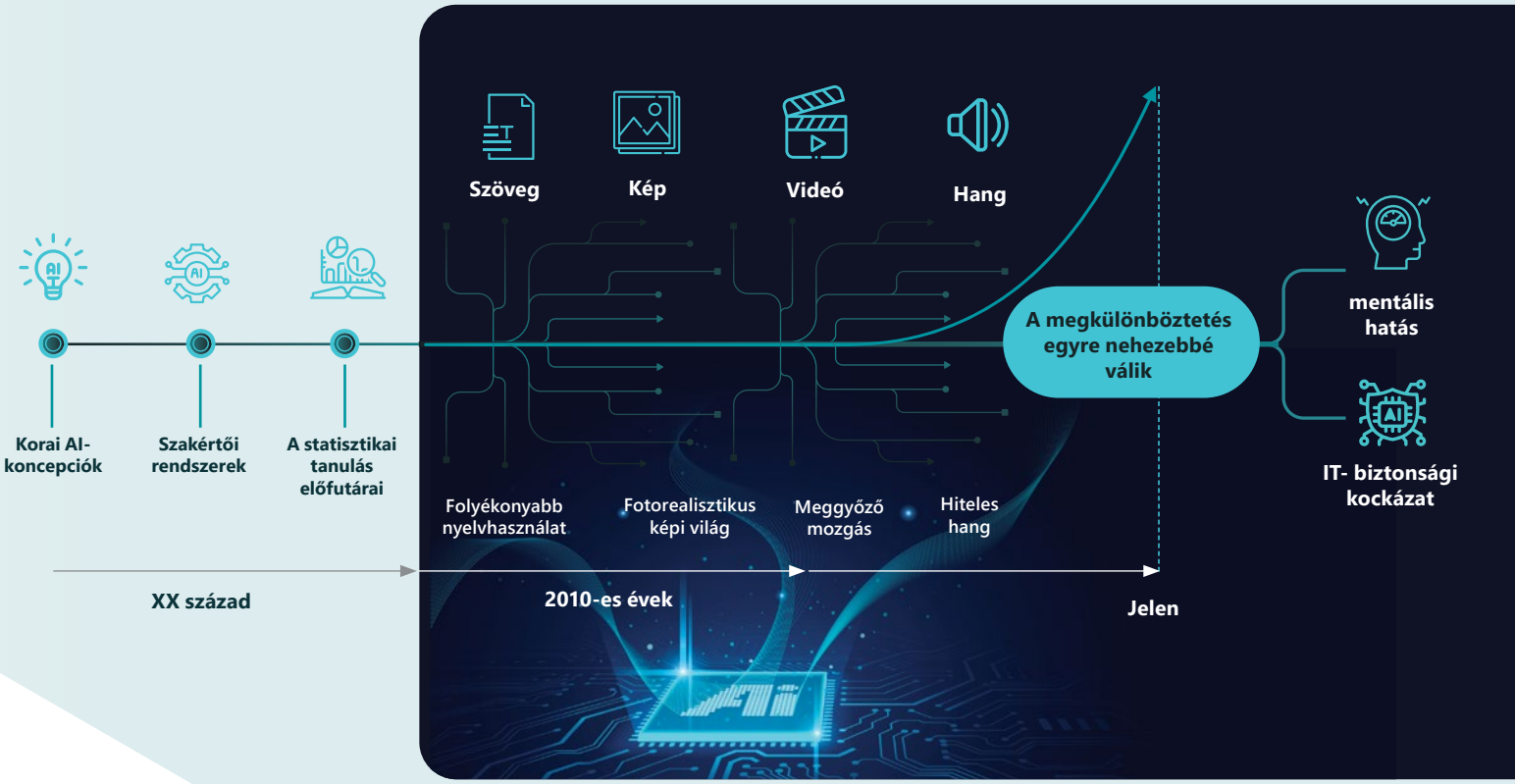
SZAKÉRTŐI KOMMENTÁR

KEREK ISTVÁN

Az elmúlt 2-3 évben jelentősen átalakult a felhasználói élmény az LLM-ek, azaz a nagy nyelvi modellek használatát tekintve. Megjelent a profi memóriakezelés, aminek következtében a felhasználók számára sokkal relevánsabb szövegeket állítanak elő a modellek és egyre komplexebben válaszolnak a feltett kérdésekre. Leegyszerűsítve, egy rövidebb, kevésbé részletes promptra is jobb válaszokat tudnak adni, mivel megtanulták, hogy melyik felhasználó hogyan értelmezi a különböző szavakat és különféle paradigma-rendszereket azonosítottak be.

Mindez beépült a kép-, és videogenerálásba is, de az LLM-ekkel való kommunikáció is teljesen új alapokra helyeződött. Ma már nem kell program kódban leírni, hogy a felhasználó mit szeretne, ahhoz, hogy a modell megértse. Egy átlagember, természetes nyelvet használva is képes használható eredményekhez jutni, mert akár 2-3 modell is működhet a háttérben, ami megfejti, hogy mire gondolt. Azaz, ami a legjelentősebb változás az AI-eszközök fejlődését tekintve az az, hogy annyiban demokratizálódott a technológia, hogy ma már nincs szükség jelentős előképzettségre ahhoz, hogy valaki jól tudja használni.

Természetesen a kreativitás, a megfelelő szakmai háttér és kritikai gondolkodás kell hozzá, ezért látunk jobb és rosszabb minőségű generált tartalmakat - ugyanakkor ma már jóval alacsonyabb belépési küszöbbel is jobb eredményeket tudnak elérni az átlagos felhasználók.



kodó hibák, ma a hihetőség sok esetben nem technikai, hanem döntési és bizalmi kérdés: a befogadónak kell eldöntenie, hogy amit lát, az dokumentáció, illusztráció vagy manipuláció.

A videogenerálás minőségi ugrását mutatja a RunwayML 2026 január 22-én megjelent kutatási összefoglalója is: saját leírásuk szerint néhány év alatt jutott el a technológia a lassan elkészülő, darabos klipektől oda, hogy az eredmény gyakran már szinte megkülönböztethetetlen a valóságtól. Mindezt megerősítik a korábban említett Microsoft Global Online Safety Survey eredményei is.

A whitepaper szempontjából a legfontosabb kérdés mégsem az, hogy „mennyire jók" ezek az eszközök, hanem az, hogy mit okoznak az egyre valósághűbb tartalmak a hétköznapi felhasználók pszichéjében. Az ESET számára készült kutatás szerint a válaszadók közel háromnegyede úgy érzi, egyre nehezebb megkülönböztetni, mi valódi, és mit készített valamilyen mesterséges intelligencia, közel minden második válaszadó pedig teljes mértékben egyetért ezzel. Ez a percepció azért kritikus, mert a megkülönböztetési bizonytalanság egyszerre lehet mentális teher (stressz és szorongás forrása, a kontrollvesztés érzésének kiváltója), és egyszerre válhat IT-biztonsági kockázati tényezővé ha egy hitelesnek tűnő üzenet vagy hívás könnyebben meggyőzi a felhasználókat.

Ezt a jelenséget külső kísérleti eredmények is alátámaszthatják. A RunwayML említett, The Turing Reel kutatásában 1043 résztvevőnek 20 darab, 5 másodperces videó alapján kellett eldöntenie, hogy valódi felvételt vagy AI-generált tartalmat lát; az összteljesítmény csak kis mértékben volt jobb a véletlennél, és csupán a résztvevők kis hányada tudott statisztikailag kiemelkedően teljesíteni. Szintén ezt erősíti a Prizma Alapítvány és az Europion által 2026 februárjában publikált kutatás, amely 1321 magyar ember megkérdezésével vizsgálta, hogy képesek-e megkülönböztetni a valódi videókat az AI-generált tartalmaktól. Az eredmény szerint a megkérdezettek csak 60 százalékban voltak erre képesek -

A következtetés a whitepaper szempontjából egyszerű: ha az átlagos felhasználók számára már nem megbízható stratégia „ránézésre" megkülönböztetni a valósat a mesterségestől, akkor a mentális és szervezeti védekezés (ellenőrzési rutinok, hitelesítési elvek, tudatosság) szerepe jelentősen felértékelődik.

A következő részben röviden bemutatjuk a kutatás módszertanát és a minta jellemzőit, hogy a whitepaperben tárgyalt jelenségek értelmezése végig átlátható, számonkérhető alapokon álljon.

> „Azt a módszert követem, hogy ha nem tudom eldönteni egy tartalomról, hogy valós-e vagy AI, akkor AI-nak tekintem"
>
> Szakértő ESET partner

Módszertan, minta, értelmezési keretek

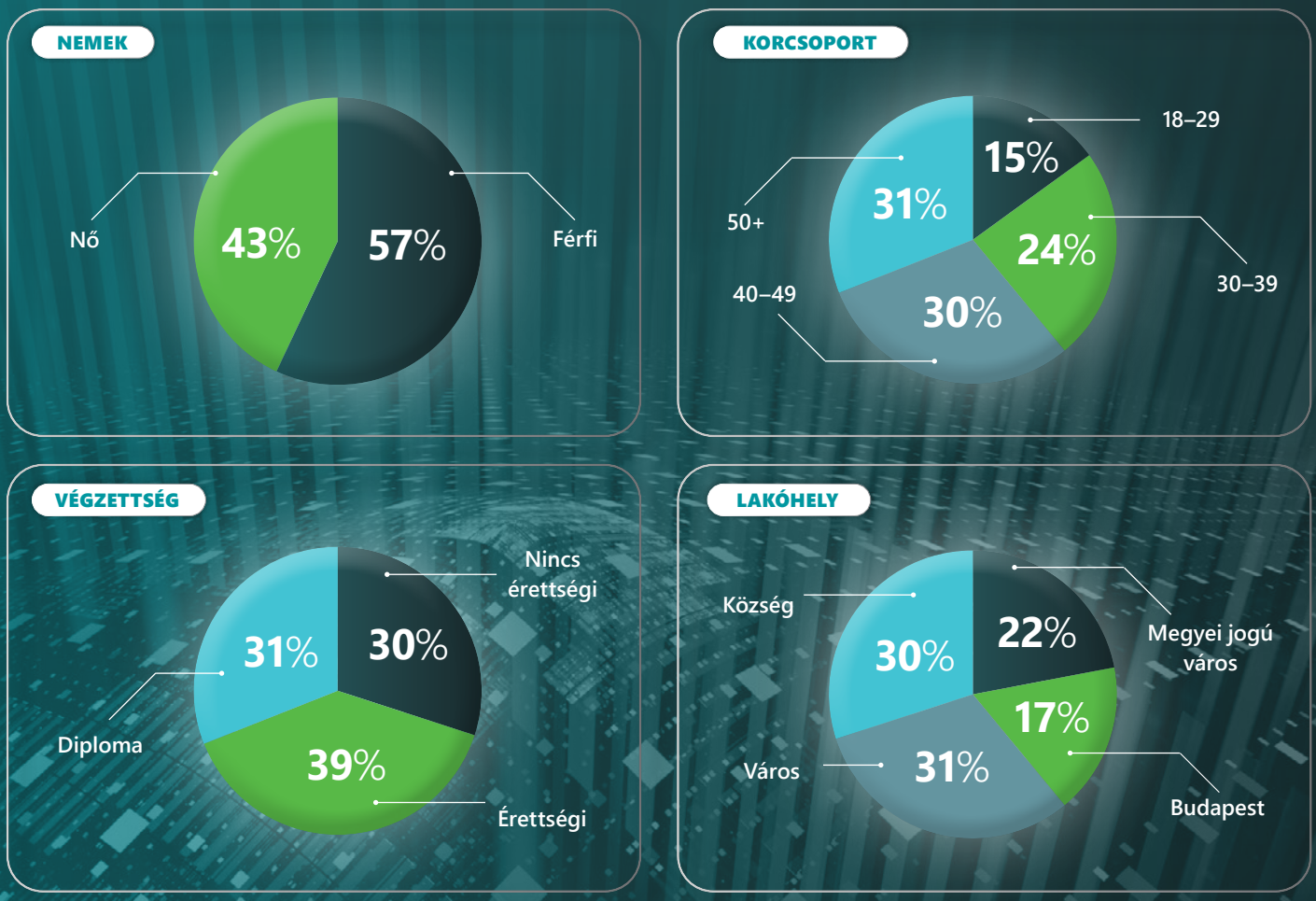
A whitepaper megállapításai egy országos, reprezentatív munkavállalói közvélemény-kutatás eredményeire épülnek. A kutatást a Medián Közvélemény-, és Piackutató szakemberei végezték az ESET magyarországi forgalmazója, a Sicontact Kft. megbízásából, kifejezetten arra fókuszálva, hogy a magyar munkavállalók hogyan viszonyulnak a mesterséges intelligenciához: milyen AI-eszközöket használnak, mire használják, milyen kockázatokat látnak és milyen mentális terheket érzékelnek a technológia terjedésével párhuzamosan.

A felmérés 600 fős véletlen mintán alapult, amely a 18 évesnél idősebb magyar munkavállalókat reprezentálja. Az adatfelvétel telefonos (CATI) interjúkkal zajlott 2025. november 25–28. között. A véletlen mintavételből adódó kisebb torzulásokat többszempontú súlyozással korrigáltuk, a Medián országos reprezentatív adatfelvételeinek munkavállalókra vonatkozó adatai alapján. A korrekciót követően a minta a magyar munkavállalók összetételét nem, életkor és végzettség szerint pontosan tükrözi. A teljes célcsoportra vonatkozó adatok hibahatára legfeljebb ±4,0%.

Fontos értelmezési szempont, hogy a kutatás önbevallásos jellegű: azt mutatja meg, hogyan látják a munkavállalók az AI-t, milyen tapasztalatokat szereztek és milyen kockázatokat érzékelnek. Ez nem technikai audit, hanem attitűdöket és észleléseket feltáró mérés. Ugyanakkor az észleléseknek gyakorlati jelentőségük van: a bizalom, a bizonytalanság és a kockázatérzet befolyásolja, hogy a munkavállalók mikor kérnek ellenőrzést, mit osztanak meg, és mennyire óvatosak a digitális csatornákon.

A következő fejezetben az AI-használat mindennapi mintázataiból indulunk ki (ki, hol, mire és milyen eszközökkel használja), mert ez adja meg azt a kontextust, amelyben az IT-biztonsági és mentális hatások értelmezhetők.

Országos, reprezentatív munkavállalói kutatás (N=600)



Telefonos (CATI) adatfelvétel 2025. november 25–28.

Elterjedtség és belépési pontok

A mesterséges intelligencia használata mára a magyar munkavállalók körében sem tekinthető rétegjelenségnek. A technológia gyorsan beépült a mindennapokba, a használati minta pedig egyértelmű: sokan privát felhasználóként kezdték el használni, majd innen szivárgott át a munkával kapcsolatos feladatokba. Ez a terjedési logika azért fontos, mert megmutatja, hogy az AI-használat sokszor nem formális vállalati döntések nyomán, hanem egyéni kísérletezésen és személyes rutinokon keresztül válik tömeges gyakorlattá.

A KUTATÁS ADATAI ALAPJÁN a válaszadók közel kétharmada, 65,1% jelezte, hogy már használt valamilyen mesterséges intelligenciát, míg 34,9% még soha. A munkahelyi megjelenés ugyanakkor ennél jóval visszafogottabb: összességében a munkavállalók 37%-a használta már a munkájához is valamelyik eszközt. A minta azt is világosan mutatja, hogy nem jellemző a kizárólag munkahelyi AI-használat: mindössze 4% mondta, hogy csak a munkájához használja, miközben 28% kizárólag magánügyben, 33% pedig egyszerre magán- és munkahelyi célokra is igénybe veszi az AI-t. Ez a megoszlás azt jelzi, hogy a munkahelyi használat sok esetben nem külön világ, hanem a már megszokott magánhasználati mintázatok folytatása.

A használat eloszlása azonban nem egyenletes, ugyanis a fiatalabbak és a magasabb végzettségűek körében az AI-használat kimagaslóan elterjedt. A kutatási adatok szerint ezekben a csoportokban 80% feletti a használat, míg a 30 év alattiak több mint fele (57%) már munkahelyi feladatokra is igénybe vett valamilyen AI-t. Eközben az idősebbek és az alacsonyabb végzettségűek óvatosabbak, de a technológia így is széles körben elérte őket: a kutatási adatok szerint majdnem minden második 50 év feletti munkavállaló kipróbálta már valamilyen formában.

> "Az ügyfeleink még sokszor minket hívnak előbb, de mi már előbb kérdezzük az AI-t, mint a Google-t"
>
> Szakértő ESET partner

A mesterséges intelligenciához való viszony jól tükrözi azokat a társadalmi törésvonalakat, amelyek más közvélemény-kérdésekben is megfigyelhetők. Minél kevésbé ismert egy jelenség – jelen esetben a generatív AI –, annál inkább társul kockázatérzettel és kontrollvesztéssel, különösen egy alapvetően bizalmatlan társadalomban, mint a magyar.

A hozzáállásbeli különbségek tehát főként az eltérő ismeretekből fakadnak: a fiatalabb, képzettebb csoportoknak gyakrabban van saját AI tapasztalatuk, ami növeli a bizalmat, míg a nem használók inkább a kockázatokat hangsúlyozzák.

A kutatás azt is mutatja, hogy sokan saját kezdeményezésre, informálisan használják az AI-t a munkájukhoz, ami egyénileg hasznos lehet, ugyanakkor a szervezetek számára kockázatokat is hordozhat.

Olyan szabályokra van tehát szükség, amelyek biztonságossá teszik az AI használatát, ugyanakkor a technológia előnyeit mindenki javára fordítják, és a hatékonyságnövekedés a munkaterhelés csökkenésében is megjelenik.

AI-HASZNÁLAT

65%
Használt már AI-t

35%
Még nem használt AI-t

37%
Munkához is használta

4%
Csak munkára használta

28%
Csak privát célokra használta

33%
Munkára és privát célokra is használta

A kép tehát kettős: vannak csoportok, ahol az AI-használat már rutinszerű, és vannak, ahol még inkább távolságtartás jellemző, de összességében a jelenség messze túlmutat a korai befogadók (early adopters) körén.

A használat belépési pontja is jól azonosítható. A válaszok alapján a leggyakoribb kapu magasan az OpenAI által fejlesztett ChatGPT. A felhasználók által megnevezett fő eszközök esetén a válaszadók 77,5%-a ezt jelölte meg első helyen. A többi megoldás jóval kisebb súllyal jelenik meg és az is látszik, hogy sokan nem kísérleteznek más eszközökkel, hanem egyetlen megszokott megoldásra támaszkodnak: a felhasználók jelentős része kifejezetten jelezte, hogy a fő AI-eszközön kívül nem használ mást. Ez a koncentráció a későbbi fejezetek szempontjából is fontos, mert a felhasználói élmény, a rutinok és a kockázatok sok esetben ugyanazok köré a platformok köré szerveződnek.

A következő oldalakon azt mutatjuk be, mire használják az AI-t a gyakorlatban: milyen feladatoknál válik mindennapi segédeszközzé és hol kezd el döntéseket, szövegalkotást vagy információfeldolgozást befolyásolni. Ez az a pont, ahol a hatékonysági ígéretek mellett érthetővé válnak a hibázási kockázatok, a túlzott bizalom jelensége és - a kutatás egyedi fókuszához kapcsolódva - a hitelességgel kapcsolatos bizonytalanság is.

SZAKÉRTŐI KOMMENTÁR — **KEREK ISTVÁN**

Mit jelent az, hogy 'használom' az AI-t? Mi a különbség a kipróbálás, az alkalmi és a tudatos használat között?
Az, hogy „használom" az AI-t, nem egy bináris állítás. A kipróbálás többnyire kíváncsiságból fakad: felteszek egy kérdést, rácsodálkozom a válaszra, de még nem épül be a munkámba.

Az alkalmi használat már praktikusabb feladatokra koncentrál, mint a fordítás, szövegellenőrzés, ötletelés, de könnyen megmarad ad hoc megoldásnak, ahol a felhasználó nem vizsgálja a forrást, nem tisztázza a kérdését, és nem ellenőrzi a kapott információt.

A tudatos, ellenőrzött beépítés ott kezdődik, hogy stratégia mentén választok eszközt, időt és képzést adok hozzá, és a tényellenőrzés szervesen beépül a munkafolyamatokba. Emellett reális elvárássá válik a kritikus gondolkodás, hogy semmit nem veszünk készpénznek, mert a végső felelősség nálunk marad. Ez azért lényeges, mert a belépési küszöb ma alacsony, kevesebb promptból is „jó" válasz jön, amit emiatt könnyű túlértékelni.

Az adatok értelmezésénél tehát számít, hogy ismerkedésről, alkalmi segítségről vagy döntéseket alátámasztó, kontrollált rutinról beszélünk.

Mire használják az AI-t a gyakorlatban?

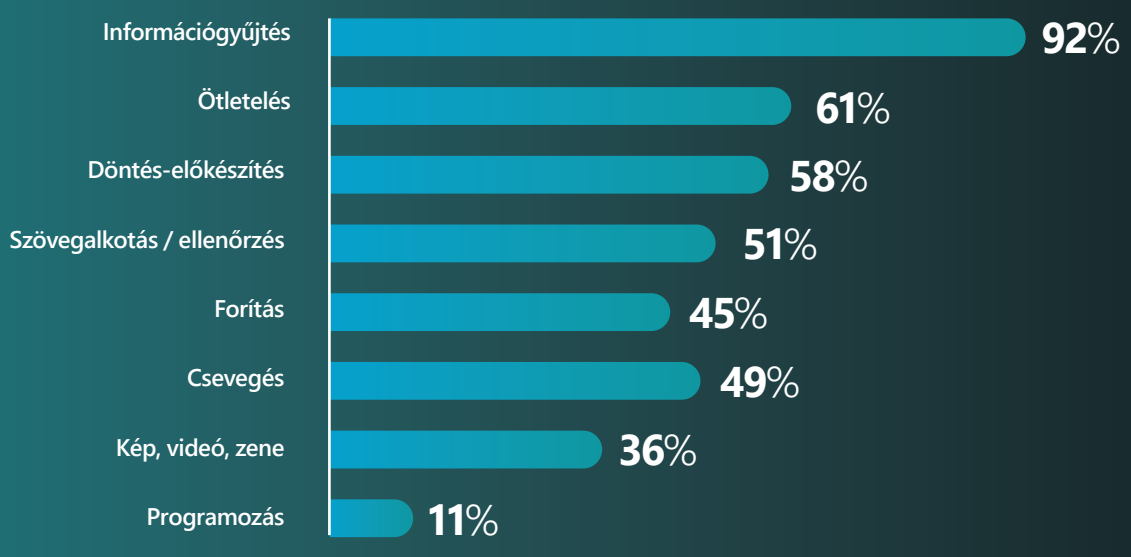
Az AI-használatra nem egyetlen tipikus forgatókönyv jellemző. A kutatás alapján a generatív eszközök leginkább olyan helyzetekben válnak mindennapi segédeszközzé, ahol tájékozódni kell, információt kell gyorsan összegyűjteni, vagy szöveget feldolgozni.

A **LÁTVÁNYOS, KREATÍV TARTALOMKÉSZÍTÉS** (kép, videó, zene) is jelen van, de a használat súlypontja inkább a nyelvhez és az információhoz kapcsolódó feladatokon van.

A felhasználási célok között toronymagasan vezet az információgyűjtés. Az AI-t használók több mint 90%-a használja keresésre és tájékozódásra, ezen belül pedig a leggyakoribb forma a vegyes használat, vagyis amikor ugyanaz a rutin jelenik meg a magáncélú és munkahelyi feladatoknál is.

Az információkeresésnél a vegyes használat aránya 45,6%, a csak magáncélú használaté 42,2%, miközben a kizárólag munkahelyi használat aránya 4,3%. Ez a kép azt sugallja, hogy az AI sokak számára nem munkahelyi eszközként indul, hanem személyes megoldásként, amelyet idővel egyre több munkával kapcsolatos helyzetben is elővesznek.

MIRE HASZNÁLJÁK AZ AI-T?



A következő legjellemzőbb kategóriák az ötletelés és a döntések előkészítése. Ötletgeneráláshoz a felhasználók 61,3%-a támaszkodik valamilyen formában AI-ra, döntés-előkészítéshez pedig 57,9%. Itt is a vegyes használat a legjellemzőbb, miközben a csak munkahelyi célú arány mindkét esetben 5% körül marad. A szövegalkotás és szövegellenőrzés szintén elterjedt, a felhasználók 51,1%-a használja ilyesmire, a kizárólag munkahelyi használat arányai itt is alacsony (7,3%). A fordítás és a „csevegés, tanácskérés" nagyjából a felhasználók felénél jelenik meg, ezeknél inkább a magáncélú használat dominál. Kép, videó vagy zene létrehozására, illetve szerkesztésére már jóval kisebb arányban vállalkoznak, itt a felhasználók körében 35,5% körüli a használat, ez jellemzően szintén magánoldalon indul. Programozáshoz az AI-t használók döntő többsége nem támaszkodik valamilyen eszközre, a használati arány 10% alatt volt az adatfelvétel időpontjában.

A magánéleti és munkacélú használat közötti „átjárás" mintázata több helyen egyértelmű. Az információval és szöveggel kapcsolatos mintázatok gyakrabban jelennek meg egyszerre olyan magán és munkahelyi céloknál, mint például a kreatív tartalomkészítés. Emellett érdemes megjegyezni, hogy a kizárólag munkahelyi használat egyik vizsgált célnál sem vált még tömegessé, jellemzően 2,5% és 7,3% közötti arányban jelenik meg. Ez a különbség fontos kontextust ad a következő részhez, ahol azt vizsgáljuk, hogyan jelenik meg mindez a szervezetekben, és milyen gyakori a spontán, szabályozatlan AI-használat.

Az eredményekhez kapcsolódó elégedettség magas. Az AI-t használók 94,0%-a alapvetően elégedett a kapott kimenettel, ugyanakkor a „mindig elégedett" válasz csak a válaszok 19,5%-ánál jelent meg. A minta egyszerre utal sikerélményre és óvatosságra. Az AI sok helyzetben elég jól működik ahhoz, hogy rutinná váljon, de a többség számára nem olyan hibátlan, hogy teljesen kiváltsa az emberi ellenőrzést. A részletekből az is kirajzolódik, hogy nem minden korcsoport használja ugyanarra a célra az AI-t, az elemzés szerint az ötletgenerálás és a szövegalkotás inkább a 30 év alattiaknál hangsúlyosabb, míg a döntések előkészítése inkább a harmincasokra és a szellemi munkakörben dolgozókra jellemző.

A következő részben ezért nem csak azt nézzük meg, hogy jelen van-e az AI a munkahelyen, hanem azt is, hogyan. Van-e szervezeti cél és keret, kapnak-e a munkavállalók tájékoztatást és képzést, és mi történik akkor, amikor a használat gyorsabban terjed, mint a szabályozás.

> **„Tapasztalatunk szerint az AI-generált tartalmak körülbelül 70–80%-ban helyesek. Egy 100 soros anyagban így nagyjából 20 sor lehet pontatlan vagy hibás, ezért minden esetben szükséges az alapos ellenőrzés"**
>
> Szakértő ESET partner

SZAKÉRTŐI KOMMENTÁR

KEREK ISTVÁN

Az AI-használat különböző módjai közti különbség és az ellenőrzés kérdése

A „keresés jellegű" AI-használat valójában információgyűjtés és rendszerezés: sok adatból összefüggéseket emel ki, rövidít, strukturál, irányt ad, de attól még nem lesz automatikusan igaz. Itt az életszerű rutin az, hogy már a kérdésben rákényszerítjük a modellt a pontosságra: tisztázzuk, mit értünk egy fogalom alatt, kérjük a források megjelölését, és a kapott állításokat visszakeressük vagy több helyről megerősítjük. Ezzel elejét vehetjük a hallucinációknak vagy kiszűrhetjük a hibás tartalmat.

A szövegalkotó használat más: akkor működik jól, ha a szerző tudja, mit akar írni, van váza és célja és az AI inkább a szerkesztést gyorsítja fel. Itt nem az a reális, hogy minden mondatot külön ellenőrzünk, hanem csak a kényes állításokat jelöljük ki, és közben figyeljük az intő jeleket, mint a túl általános, közhelyes, vagy szakmai pontatlanságokat tartalmazó szöveg.

A döntéstámogató használatnál a legszigorúbb a kontroll, mert itt már következménye van annak, ha egy információ félremegy. Ebben az esetben a minimum, hogy semmit sem veszünk készpénznek: a modell csak előkészít, a végső felelősség a felhasználónál marad. Itt kulcsfontosságú a kritikus gondolkodás, valamint a tények, a kontextus figyelembe vétele és az alternatív magyarázatok keresése.

Munkahelyi használat, kommunikáció és képzés

Ahogy a korábban említett adatokból kitűnik, a munkahelyi AI-használat egyik legfontosabb jellemzője, hogy sokszor nem egy szervezeti döntés következményeként jelenik meg, hanem alulról építkezik. Emiatt jellemzően később születnek meg azok a keretek, amelyek kijelölik a célokat, a felelősséget és a biztonságos használat határait.

A KUTATÁSI ADATOK ALAPJÁN az AI-t használók körében a munkahelyi alkalmazás jellemzően nem a munkáltató által biztosított eszközhöz kötődik. A mesterséges intelligenciát munkára is használók között mindössze 11% jelezte, hogy a munkaadó által biztosított eszközt használja, miközben 65,3% saját kezdeményezésből nyúlt a technológiához. A megkérdezettek 23,7%-a pedig egyáltalán nem használ a munkájához AI-t. Ez a megoszlás arra utal, hogy a munkahelyi használat sokszor nem intézményesített, hanem személyes döntésekből fakad, emiatt kevésbé átlátható, nehezebben kontrollálható.

A szervezeti kommunikáció hiánya is ezt a képet erősíti. A válaszadók 79,7%-a szerint a munkahelyén hivatalosan eddig nem volt szó az AI bevezetéséről vagy használatáról és csak 17,6% tapasztalta ennek ellenkezőjét. Azonban az, hogy egy szervezetben még nem került szóba az AI bevezetése, nem feltétlenül jelenti, hogy a technológiát ne használnák a szervezet tagjai. Inkább azt mutatja, hogy a technológia megjelenése és az erről szóló szervezeti párbeszéd nem mindig jár együtt. Ilyenkor könnyen kialakul egy olyan átmeneti állapot, amelyben a munkatársak már elkezdik használni az új technológiai eszközöket, de közben még nem világos, mit tekint a szervezet helyes gyakorlatnak, és mi számít kockázatosnak.

Ahol a téma már felmerült, ott is vegyes a kép. Azok közül, akik szerint a munkahelyen volt szó AI-ról, 60,8% jelezte, hogy tájékoztatták őket arról, mi a munkáltató célja a bevezetéssel, 39,2% viszont nem kapott ilyen magyarázatot. Ez a különbség nem pusztán kommunikációs kérdés: ha a célok nincsenek tisztázva, a használat ad hoc módon, egyéni értelmezések és szokások alapján alakul, és nehezebben kapcsolható össze minőségi elvárásokkal, adatkezelési szabályokkal vagy ellenőrzési rutinokkal.

A képzésnél még élesebb a kontraszt. Azokban a munkahelyi helyzetekben, ahol az AI egyáltalán szóba került,

AI-HASZNÁLAT

Igen Nem

Volt-e szó hivatalosan AI-használatról a munkahelyen?

Tájékoztatták-e az AI-használat céljáról?

Kapott-e képzést az AI-használathoz?

A használat gyakran megelőzi a kereteket

a válaszadók 34,2%-a kapott valamilyen AI-használati képzést, 65,8% viszont nem. A képzés hiánya autodidakta tanulást eredményez, ami azzal a veszéllyel jár, hogy megjelenik a Dunning-Krueger hatás, az a kompetencia illúzió, ami a hiányzó tudást nárcisztikus megelégedettséggel pótolja. Ugyanakkor a képzés iránti igények megítélése erős: ugyanebben a körben 49% nagyon fontosnak, 37,1% inkább fontosnak tartja, hogy a dolgozók AI-használatról képzést kapjanak. Vagyis a kutatás szerint nem közönyös témáról van szó, a többség érzi, hogy az AI használata új készségeket, új felelősséget és új döntési helyzeteket hoz.

A munkahelyi terjedés egyik jellegzetes kísérőjelensége, hogy a munkavállalók nagy része magától próbál rájönni arra, hogyan érdemes használni az eszközöket. Az AI-t használók közel 31%-a már kért segítséget valakitől, leggyakrabban családtagtól, baráttól vagy munkatárstól. Ez az adat annak fényében érdekes, ha úgy is értelmezzük, hogy 69% nem kért információt a környezetétől. Ennek az a veszélye, hogy ez a csoport úgy gondolja, hogy csinál valamit, miközben nem érti a működés lényegét. Ez a közösségi tanulási minta természetes, de nem pótolja a szervezeti iránytűt, különösen ott, ahol érzékeny adatok, belső folyamatok vagy döntéstámogatás kerül a képbe.

A következő részben innen lépünk tovább az AI használatának IT-biztonsági vetületeihez. Ha a használat sokszor saját kezdeményezésből történik, a célok nem mindig tiszták, és a képzés hiányos, akkor érthető, miért válik központi kérdéssé a bizalom, az adatmegosztás, az ellenőrzés és a megtéveszthetőség. A szervezeti keretek hiánya nem csak szabályozási kérdés, hanem közvetlen kockázati tényező is.

SZAKÉRTŐI KOMMENTÁR

CSIZMAZIA-DARAB ISTVÁN

Miért kockázatos a csendes terjedés, és mi a legkisebb, még reális szervezeti minimum a felkészüléshez? Ahogy a kutatásból is kiderült, gyakori jelenség, hogy a munkavállalók a „saját szakállukra" kezdenek kísérletezni az AI-eszközökkel, ami viszont jelentős adatvédelmi kockázatokat hordoz egy szervezet számára.

Az emberek gyakran a legkisebb ellenállás irányába mennek, ezért előfordulhat, hogy a saját életük megkönnyítése érdekében megpróbálják megkerülni a biztonsági szabályzatokat. Ez komoly probléma, mert tudatos használat nélkül könnyen támadhatóvá válnak a munkahelyi informatikai rendszerek.

A cégeknek ezért erős biztonsági intézkedéseket kellene betartatniuk, amelyeket a működésük sajátosságaihoz igazítanak. A munkavállalók esetén pedig kulcsfontosságú lenne az élethosszig tartó autodidakta tanulás, biztonságtudatossági képzés és a kritikai gondolkodás megerősítése is.

Bizalom, ellenőrzés, adatmegosztás:

Miért lesz az AI egyszerre eszköz és kockázati tényező?

A generatív AI használata ma már nem pusztán technológiai kérdés. Olyan eszközzé vált, amelyhez a felhasználók gyakran javaslatért, összefoglalóért vagy döntéseket segítő szempontokért fordulnak.

SZAKÉRTŐI KOMMENTÁR — **KELETI ARTHUR**

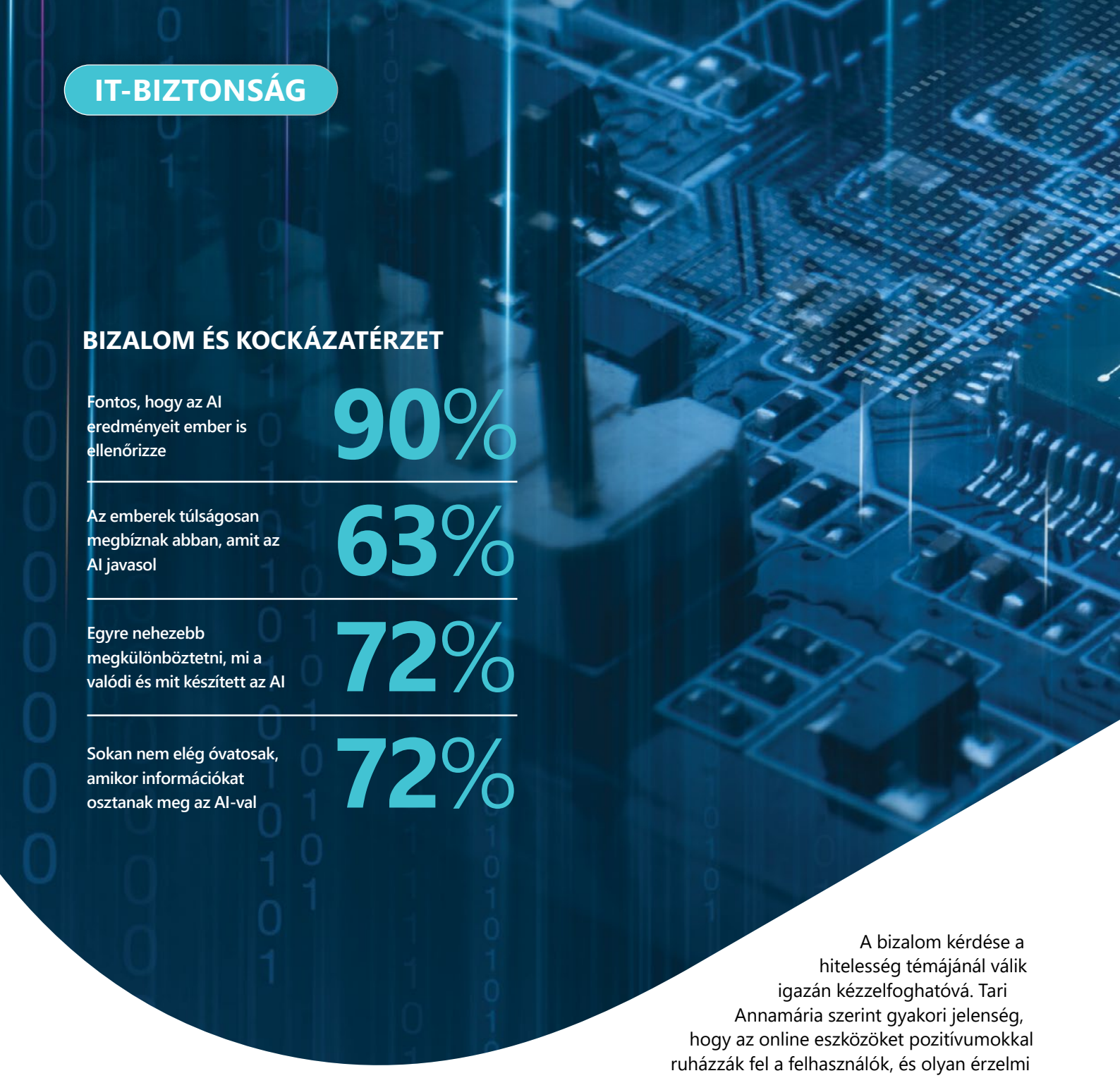
Miért válik a bizalom szervezeti szintű kérdéssé, és miért nem lehet kizárólag egyéni óvatosságra építeni?
A generatív AI elterjedésével a bizalom többé nem pusztán személyes óvatosság kérdése, hanem egyéni és szervezeti támadási felület.

Ha az írott szöveg és főleg a hang már teljesen valósághű, illetve ha már az összes érzékszervünk "elesik" az AI-tartalmakkal szemben, akkor az egyéni megérzésre építő védekezés összeomlik: hiába „hallom a saját fülemmel" a főnököm hangját, a hallott jel önmagában már nem bizonyíték. Ráadásul az AI-asszisztensek egyre több mindent intéznek a nevünkben, hozzáférnek az erőforrásainkhoz, míg a másik oldalon rosszindulatú szereplők vagy agentek képesek velük „tárgyalni", információt kicsalni vagy valamilyen utasítást becsempészni (prompt injection) a működésükbe. Ilyen környezetben nem várható el, hogy minden munkatárs állandóan azonosítson, jelszavazzon, gyanakodjon, mert a munka és az emberi kapcsolatok nem erre vannak berendezkedve.

A bizalom ezért szervezeti szintű kereteket igényel: kontextus-alapú, dinamikus hozzáférés (miért, mihez, meddig), intenzív naplózás és ellenőrzés, teljes tiltás helyett pedig olyan vállalati megoldások biztosítása, amit a dolgozók ténylegesen használhatnak és amely számukra szinte láthatatlanul védi meg őket.

EMIATT AZ AI KÖRÜLI KOCKÁZATOK jelentős része nem abból fakad, hogy „hibázik-e a rendszer", hanem abból, hogy mekkora bizalommal fogadjuk az eredményt, mennyire ellenőrizzük azt, és milyen információkat adunk át az AI-rendszereknek.

A kutatás egyik legerősebb jelzése, hogy az emberi ellenőrzés igényével kapcsolatban szinte teljes a konszenzus. A válaszadók döntő többsége egyetért azzal, hogy az AI által adott eredményeket és javaslatokat embernek is ellenőriznie kell. Ez a hozzáállás egyszerre józan és reális. A felhasználók érzik, hogy az AI hasznos techno-



BIZALOM ÉS KOCKÁZATÉRZET

Fontos, hogy az AI eredményeit ember is ellenőrizze **90%**

Az emberek túlságosan megbíznak abban, amit az AI javasol **63%**

Egyre nehezebb megkülönböztetni, mi a valódi és mit készített az AI **72%**

Sokan nem elég óvatosak, amikor információkat osztanak meg az AI-val **72%**

lógia, de nem tekintik tévedhetetlennek. A kontroll igénye tehát jelen van, ugyanakkor a mindennapi rutinokban mégis gyakran előfordulhat, hogy az ellenőrzés elmarad, főként, ha a kimenet elsőre meggyőzőnek tűnik.

Ezzel összefügg az a jelenség is, hogy sokan túlzottan megbíznak abban, amit az AI javasol. A kutatás alapján ez nem marginális vélekedés, hanem széles körben megjelenő tapasztalat. Fontos, hogy ez nem feltétlenül önkritika, sokkal inkább a környezet megfigyelése. A következménye viszont ugyanaz; ha a felhasználók hajlamosak az AI által generált tartalmakat megbízhatóként elfogadni, az önmagában kockázati tényezővé válhat, különösen akkor, ha a válaszok döntéseket, pénzügyi lépéseket vagy munkafolyamatokat befolyásolnak.

A bizalom kérdése a hitelesség témájánál válik igazán kézzelfoghatóvá. Tari Annamária szerint gyakori jelenség, hogy az online eszközöket pozitívumokkal ruházzák fel a felhasználók, és olyan érzelmi kapcsolatot alakítanak ki, amelyet észre sem vesznek. A kutatás szerint a válaszadók többsége úgy érzi, egyre nehezebb megkülönböztetni, mi valódi, és mit készített mesterséges intelligencia. Ez a bizonytalanság két irányban hat: egyrészt mentális teherként jelenhet meg, mert a hétköznapi tájékozódás alapját a bizalom adja, és ha ez meginog, az stresszt és kontrollvesztés-érzést okozhat. Másrészt biztonsági kockázati tényező, mert a megtévesztés annál könnyebben működik, minél valószerűbb és minél kevésbé ellenőrzött a tartalom.

Az adatmegosztással kapcsolatban is jelentős a kockázat érzete. A válaszadók jelentős része úgy látja, hogy az emberek nem elég óvatosak, amikor információkat osztanak meg

„Tilos a személyes adatok betöltése az AI-ba, speciális konfigurációs adatokat sem adhatnak meg a kollégák”

Szakértő ESET partner

az AI-eszközökkel. Ez az óvatosság különösen a munka világában kritikus, hiszen itt nemcsak személyes adatok, hanem belső dokumentumok, ügyfél-információk, üzleti tervek és folyamatleírások is a „megosztható” tartományba csúszhatnak, ha nincs világos szervezeti iránymutatás. A kutatás logikája ezen a ponton egyszerű: ha a felhasználók bizonytalanok abban, mit szabad megosztani, akkor a legkisebb kényelmi döntés is kockázattá válhat.

A felhasználói percepciók az AI munkahelyi hatásaival kapcsolatban sem semlegesek. A munkahelyek átrendeződésének feldolgozása jelentős energiát és rugalmasságot igényel, míg a munkahely elvesztésének lehetősége összefonódik az értéktelenség érzésével. A kutatásban megjelenik az az állítás is, hogy az AI használata miatt támadhatóbbak lehetnek a munkahelyi informatikai rendszerek, ahogy az is, hogy az AI használata nagyobb egyéni felelősséget ró a munkavállalókra, mint korábban. Ez a két gondolat összekapcsolódik. Ha a használat gyorsan terjed, és közben a szabályok, a képzés, valamint az ellenőrzési rutinok nem alakulnak ki elég gyorsan, akkor a kockázat nemcsak technikai, hanem szervezeti és emberi tényező is.

A következő részben innen lépünk tovább a megtévesztés témájára. Ha a hitelesség megítélése nehezebb, ha a felhasználók szerint sokan túlzottan bíznak az AI-ban, és ha az információmegosztás körül bizonytalanság van, akkor érthető, miért válik hangsúlyossá az életszerű, AI-val támogatott social engineering, legyen szó e-mailről, telefonhívásról vagy hangalapú megszemélyesítésről.

SZAKÉRTŐI KOMMENTÁR

CSIZMAZIA-DARAB ISTVÁN

Milyen információk tekinthetők tipikusan érzékenynek, miért nem mindegy, hová kerülnek, és mi az a minimális óvatosság, ami a mindennapi gyakorlatban reálisan elvárható?

Érzékeny adat minden, amivel konkrétan beazonosíthatók vagyunk: például név, lakcím, születési adatok, igazolványszámok. Kiemelten fontosak a pénzügyi adataink (kártyaszám, CVV kód, jelszavak), egészségügyi adataink és tartózkodási helyünk.

Tekintsük az adatainkat értéknek! Ezek illetéktelen kezekbe kerülése komoly veszélyekkel járhatnak, amelyek a pillanatnyi kellemetlenségtől kezdve akár komoly pénzügyi veszteségekig is terjedhetnek. Az ellopott bizalmas adatokkal zsarolhatnak bennünket, profilunk feltörésével ismerőseinket is becsaphatják.

A minimális óvatosság alapja az informatikai higiénia. Használjunk egyedi, erős jelszavakat, tároljuk ezeket jelszókezelőben, és mindenhol aktiváljuk a kétfaktoros hitelesítést (2FA).

Alkalmazzunk eszközeinken naprakész vírusvédelmet, valamint telepítsük azonnal a hibajavító szoftverfrissítéseket a kihasználható sebezhetőségek bezárására. Kezeljünk minden kéretlen megkeresést egészséges gyanakvással, és adataink megadása előtt gondoljuk át mindig a lehetséges a kockázatokat.

AI-JAL TÁMOGATOTT MEGTÉVESZTÉS

Hogyan lesz valósághűbb a social engineering?

A megtévesztés nem új jelenség az IT-biztonság világában. A social engineering lényege eddig is az volt, hogy a támadók nem a rendszereket, hanem az embereket próbálják megkerülni, kijátszani, úgy, hogy a célpont bizalmára, rutinjaira és pillanatnyi figyelmére hatnak.

MI AZ AI TERJEDÉSÉVEL MEGVÁLTOZIK, AZ NEM MAGA AZ ALAPELV, hanem az eszköztár minősége és skálázhatósága. A generatív megoldások képesek fokozni a meggyőzéshez használt tartalmak minőségét, ezzel pedig olyan üzeneteket vagy kéréseket is hihetőbbé tehetnek, amelyek korábban jobban kilógtak a sorból.

A kutatás adatai azért különösen fontosak ezzel a kérdéssel kapcsolatban, mert azt mutatják, hogy a felhasználói oldalon már most is erős a bizonytalanság és a kockázatérzet. A válaszadók 90%-a egyetért azzal, hogy az AI eredményeit embernek is ellenőriznie kell. Ugyanakkor a többség azt is érzékeli, hogy a gyakorlat sokszor eltér az ideális elvtől. A megkérdezettek 63%-a szerint az emberek túlságosan megbíznak abban, amit az AI javasol, 72% szerint pedig egyre nehezebb megkülönböztetni, mi a valódi, és mit készített AI. Ezek az észlelések együtt egy olyan környezetre utalnak, ahol az életszerűség, valósághűség önmagában rizikófaktorrá válhat, mert a hitelesség megítélése nehezebb, miközben a döntési helyzetek gyorsak és gyakran rutinszerűek. Az AI eredményeibe vetett hit

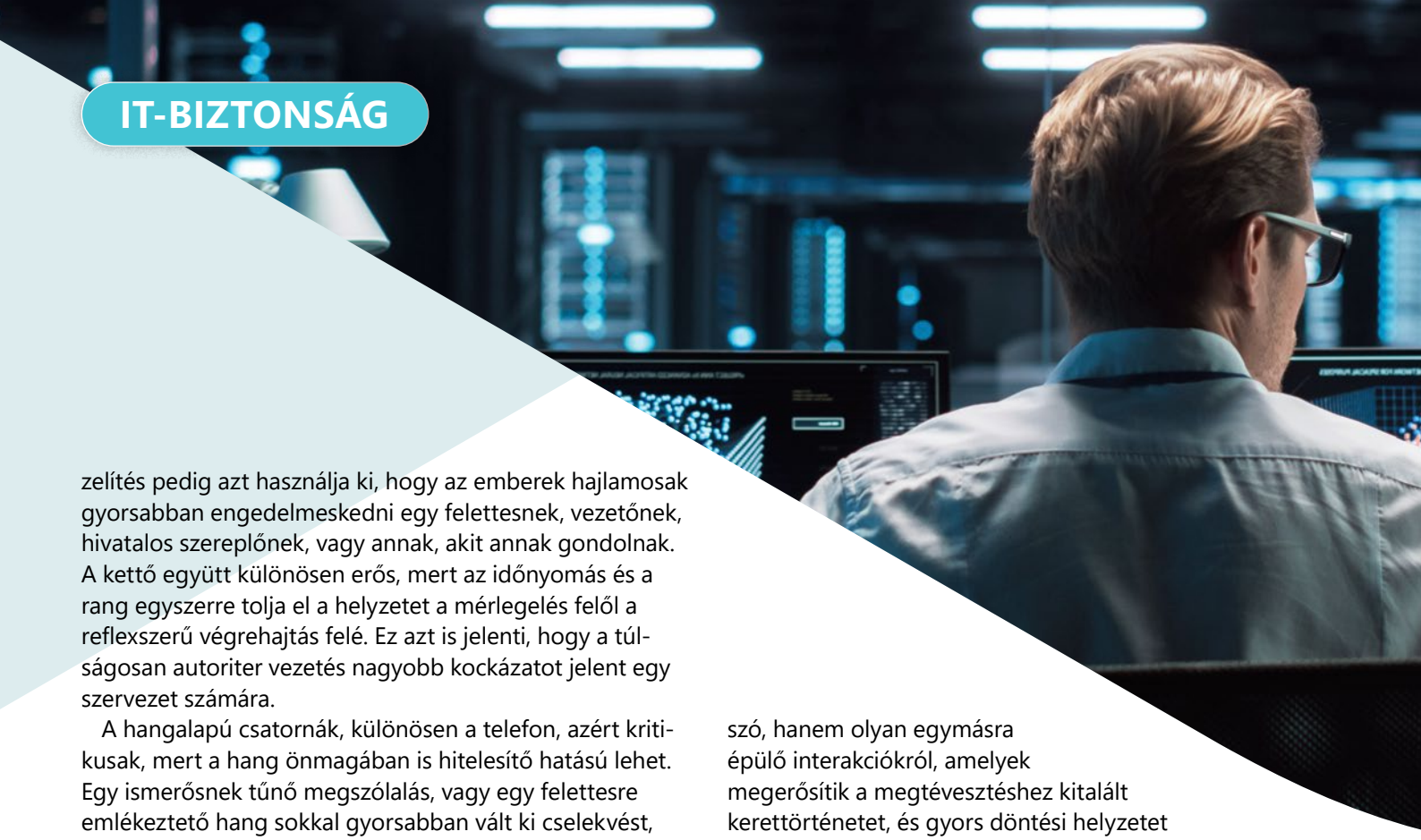
Védekezési minimum: visszaellenőrzés, hitelesítés, jóváhagyás

sokszor önmagában olyan érzelmi idealizációt feltételez, ami szoros összefüggésben áll a bizalommal és a naivitással.

A megtévesztési kísérletek egyik klasszikus terepe az e-mail és az üzenetküldő csatornák világa. Itt az AI szerepe elsősorban abban ragadható meg, hogy a támadók által használt tartalom nyelvileg kifinomultabb, következetesebb, sőt akár személyesebb hatású lehet, miközben gyorsabban és több változatban előállítható. Ez azért fontos, mert a felhasználók gyakran a nyelvi minőségből, a stílusból, illetve a szokatlan nyelvi fordulatokból következtetnek arra, hogy gyanús-e egy üzenet. Ha ezek a kapaszkodók gyengülnek, az ellenőrzés még fontosabb szerephez jut.

A social engineering hatékonyságát hagyományosan két pszichológiai eszköz képes kifejezetten erősen támogatni, a sürgetés és a tekintély hatása. A sürgetés lényege, hogy a célpontot időnyomás alá helyezi, ezzel csökkentve az ellenőrzés valószínűségét vagy alaposságát. Ilyenkor a kérés általában úgy van megfogalmazva, hogy „most kell lépni”, vagy úgy, hogy felvesse a késlekedés azonnali következményeinek kockázatát. A tekintélyre építő megkö-

> **„Több olyan támadásról is hallottunk már, ahol például a pénzügyi vezető hangját másolták le és így kértek utalást valamelyik beosztottól”**
>
> Szakértő ESET partner



zelítés pedig azt használja ki, hogy az emberek hajlamosak gyorsabban engedelmeskedni egy felettesnek, vezetőnek, hivatalos szereplőnek, vagy annak, akit annak gondolnak. A kettő együtt különösen erős, mert az időnyomás és a rang egyszerre tolja el a helyzetet a mérlegelés felől a reflexszerű végrehajtás felé. Ez azt is jelenti, hogy a túlságosan autoriter vezetés nagyobb kockázatot jelent egy szervezet számára.

A hangalapú csatornák, különösen a telefon, azért kritikusak, mert a hang önmagában is hitelesítő hatású lehet. Egy ismerősnek tűnő megszólalás, vagy egy felettesre emlékeztető hang sokkal gyorsabban vált ki cselekvést, mint egy e-mail, mert a beszélgetés élő helyzetet teremt, és a felhasználó gyakran kisebb eséllyel áll meg ellenőrizni. Különösen, ha az ellenőrzés abból állna, hogy az adott vezetőt kell megkérdezni, hogy valóban ő telefonált-e. Egy ilyen kérdés sokakat elbizonytalaníthat, mert ha nem indokolt, akkor a kérdező személyét akár le is értékelheti a vezetőség szemében. A kutatásban a kockázatérzet ezzel összhangban megjelenik. A válaszadók 72%-a szerint sokan nem elég óvatosak, amikor információkat osztanak meg az AI-jal, és több mint felük egyetért azzal is, hogy az AI-használat miatt támadhatóbbak lehetnek a munkahelyi informatikai rendszerek. A két állítás együtt arra utal, hogy a felhasználók már most érzékelik az emberi tényező felértékelődését, még akkor is, ha a konkrét támadási formákat nem mindig tudják pontosan megnevezni.

A megtévesztést tovább erősítheti, ha több csatorna egymást „hitelesíti". Ilyenkor nem egyetlen üzenetről van szó, hanem olyan egymásra épülő interakciókról, amelyek megerősítik a megtévesztéshez kitalált kerettörténetet, és gyors döntési helyzetet teremtenek. Ez az a pont, ahol a szervezeti rutinok válnak döntővé. Ha a hitelesség megítélése egyre nehezebb, akkor a védekezés nem épülhet kizárólag arra, hogy valaki „kiszúrja a gyanús jeleket". Olyan egyszerű, ismételhető gyakorlatokra van szükség, amelyek természetes módon beépülnek a mindennapokba, például a visszaellenőrzés kultúrájára, a külön csatornán történő megerősítésre, illetve a pénzügyi vagy hozzáférési jellegű kérések szigorú jóváhagyási rendjére.

A következő részben ezért azt nézzük meg, milyen szervezeti minimumok segíthetnek abban, hogy az AI-t a munkában is biztonságosan lehessen használni. A cél nem az, hogy a felhasználók féljenek a technológiától, hanem az, hogy az egyre valósághűbb tartalmak korában a bizalom mellé újra kiépüljön az ellenőrzés, a hitelesítés és a felelősség rendszere.

SZAKÉRTŐI KOMMENTÁR

TARI ANNAMÁRIA

Egy munkahelyen a vezetők és az alkalmazottak is szorongással reagálhatnak az AI immerzív és szinte követhetetlenül gyors megjelenésére. A cégek versenyhelyzetbe kényszerülnek, egymást kergetik egy olyan terepen, ahol egyelőre olykor több a kérdés, mint a biztos válasz. Optimális helyzetben a kölcsönösség, a tiszta és átlátható kommunikáció, a megbecsülés összetartja a céget, még nehéz helyzetekben is. De az AI által teremtett szituációk - például amikor a vezető sem biztos, hogy többet tud az alkalmazottnál - ideális táptalajt teremt az inkompetenciától való félelem számára.

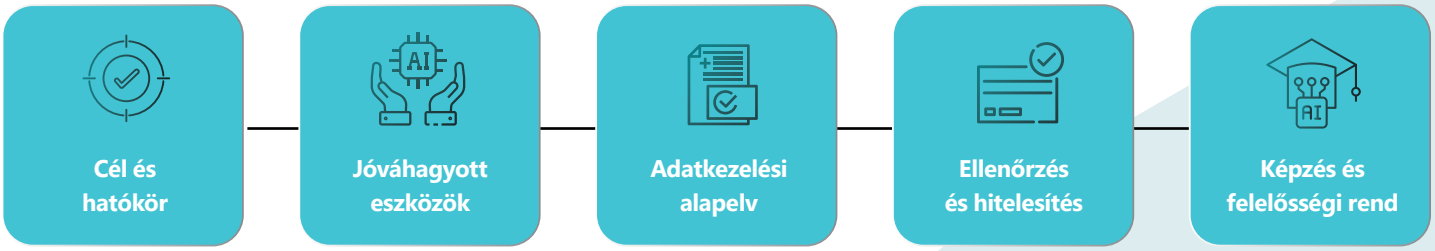
Előfordulhat, hogy a felsővezető féken tartott szorongása „lecsorog" az alkalmazottak közé, akik szintén szorongani kezdhetnek. Ez abból fakad, hogy állandóan figyelniük kell rá, hogy mindent jól csinálnak-e, változtatniuk kell-e valamin, illetve hogy valóban a legfrissebb információkhoz férnek-e hozzá az AI-jal kapcsolatban. Ha egy vezető a tekintélyéhez valójában szorongás is kapcsolódik, akkor az alkalmazottak ott is sürgető helyzeteket fognak észlelni, ahol nem lenne szükséges.

A legfontosabb, hogy az inkompetenciától való félelmet, ha nem is kommunikálják teljesen nyíltan, de legalább ismerjék el a vezetőség tagjai is. Ez az érzelmi helyzet teremthet akkora bizalmat, hogy az alkalmazott nem csúszik olyan döntések felé, amit nyugodt állapotban kritikai szűrő alá venne.

SZERVEZETI VÁLASZOK

Milyen keretek csökkentik az AI-jal kapcsolatos kockázatokat?

A munkahelyi AI-használat terjedése alapján ma már nem az a kérdés, hogy lesz-e AI a szervezetekben, hanem az, hogy milyen módon lesz jelen.

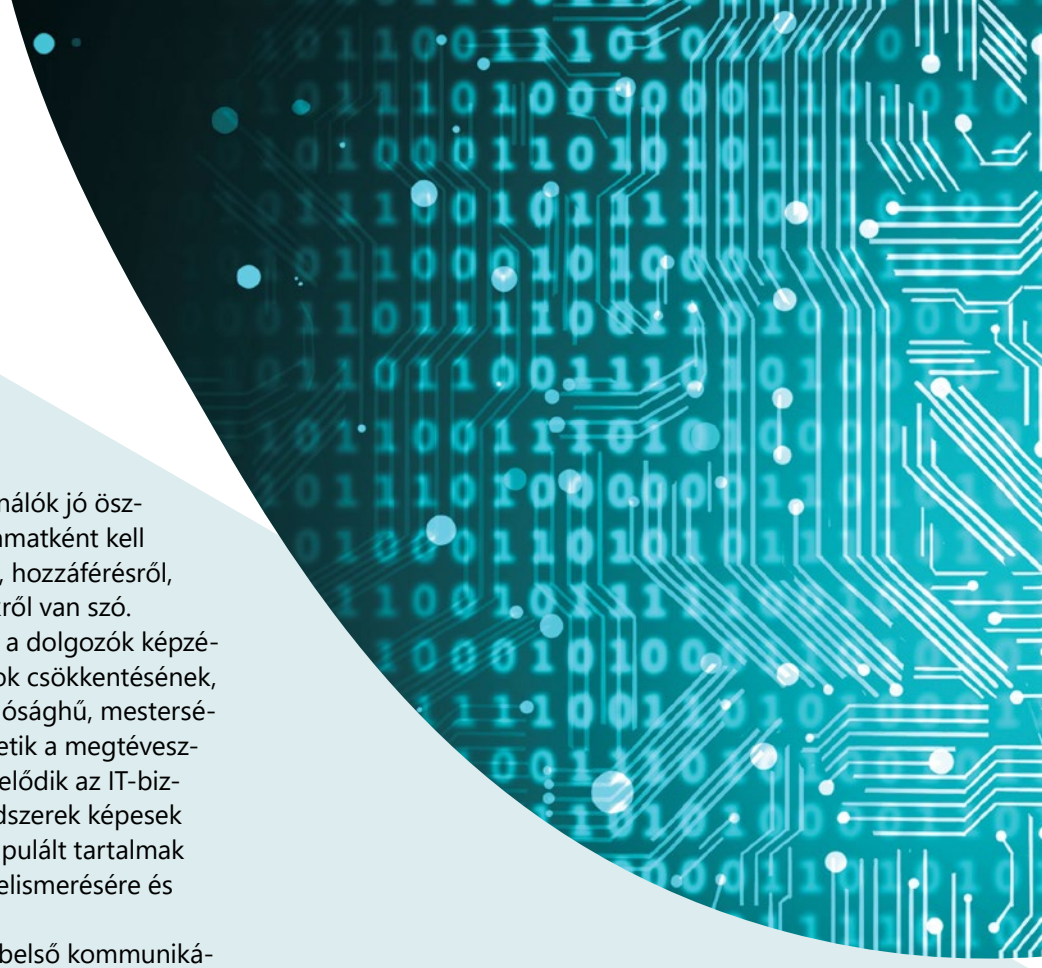


A KUTATÁS AZT MUTATJA, HOGY A FELHASZNÁLÓK SOK ESETBEN SAJÁT KEZDEMÉNYEZÉSBŐL nyúlnak ezekhez az eszközökhöz, miközben a szervezeti keretek, a célok és a képzés gyakran később jelennek meg. Ebben a helyzetben a legnagyobb rizikófaktor nem maga a technológia, hanem az, ha a használat úgy válik rutinná, hogy közben nincs közös iránytű.

Az első szervezeti minimum a cél és a hatókör tisztázása. Egyszerűen meg kell fogalmazni, hogy a szervezet mire szeretné használni az AI-t, és mire nem. Ha a célok nincsenek kimondva, a használat szerteágazóvá válik, és nehezebb megítélni, mi számít jó gyakorlatnak. Nem részletes szabályzatokkal érdemes kezdeni, hanem világos alapelvekkel. Ilyen lehet például, hogy milyen típusú feladatoknál elfogadott az AI használata, és melyek azok a helyzetek, ahol különösen nagy óvatosság szükséges.

A következő alapelv az eszközök és az adatok kérdése. Nem mindegy, milyen felületre kerül a tartalom, és az sem mindegy, milyen információt oszt meg a felhasználó egy AI-rendszerrel. Ezért szükség van egy közérthető, mindennapi munkára lefordítható adatkezelési minimumra. A lényege nem jogi szöveg, hanem gyakorlati döntési segédlet: mik azok az információk, amelyeket semmiképp nem szabad beírni vagy feltölteni, és milyen típusú tartalom kezelhető biztonságosabban. Ha ez nincs tisztázva, az óvatosság egyéni megérzésekre épül, és könnyen ingadozóvá válik.

A harmadik pillér az ellenőrzési és hitelesítési rutinok beépítése. Az AI-jal támogatott megtévesztések esetében különösen



fontos, hogy a szervezetek ne a felhasználók jó ösztöneire építsenek. A hitelesítésnek folyamatként kell működnie, különösen akkor, ha pénzről, hozzáférésről, adatok kiadásáról vagy sürgető kérésekről van szó.

A technológiai védelmi rendszerek és a dolgozók képzése egyaránt alapvető pillére a kockázatok csökkentésének, a szervezeti folyamatokkal együtt. A valósághű, mesterségesen generált tartalmak megkönnyíthetik a megtévesztésre épülő támadásokat, ezért felértékelődik az IT-biztonsági rendszerek szerepe. Ezek a rendszerek képesek lehetnek a gyanús kommunikáció, manipulált tartalmak vagy rosszindulatú fájlok automatikus felismerésére és szűrésére.

Ugyanilyen fontosságú a képzés és a belső kommunikáció, amelyek a szervezeti tudatosságot és az alapvető ellenőrzési rutinok elsajátítását biztosítják. A kutatás alapján ott, ahol felmerül az AI bevezetése, a dolgozók többsége fontosnak tartja, hogy kapjanak képzést, ennek ellenére ez gyakran elmarad. A képzés nem azt jelenti, hogy minden munkavállalót szakértővé kell tenni, hanem azt, hogy legyen közös nyelv az alapfogalmakra, érthető példák a tipikus kockázatokra, és egyszerű ellenőrzési rutinok, amelyekre rá lehet szokni.

A működőképességhez felelősségi rend is kell. Ha a felhasználó bizonytalan, jó, ha tudja, hova fordulhat kérdéssel és mi a teendő, ha gyanús megkeresést kap. A felelősségi rend nem feltétlenül új szervezeti egységet jelent, sokkal inkább kijelölt szerepköröket, elérhető kontaktpontokat és egy rövid, világos közös protokollt. Ugyanez igaz az incidensek jelzésére is: a gyors reakció esélyét növeli, ha a jelzés útja egyszerű, és nem jár bürokratikus terhekkel.

A szervezeti kereteknek van egy további, gyakran alulértékelt hatása is. Nem csak az IT-biztonsági kockázatokat csökkentik, hanem a bizonytalanságot is. Ha a felhasználók tudják, mi a cél, mi fér bele, mi nem, és mihez kell visszaellenőrzés, az csökkentheti a kontrollvesztés érzését. Ez a szempont már átvezet a következő fejezethez, amely az AI-használat mentális hatásait vizsgálja.

SZAKÉRTŐI KOMMENTÁR

KELETI ARTHUR

A legkisebb szervezeti minimum nem egy százoldalas tiltólista, hanem néhány olyan alaplépés, ami nélkül az egész szétcsúszik. Először is fel kell térképezni az informatikai helyzetet, mert ahol a shadow AI megjelenik, ott szinte biztosan shadow IT-ról is beszélhetünk. Fel kell tárni, hogy, mit használnak a kollégák, amit nem kellene, és érdemes megvizsgálni azt is, hogy ezeket az eszközöket pontosan mire használják a munkájuk során. Ez azért elengedhetetlen, mert ha egy cégnek nincs képe a valóságról, semmit sem tud jól szabályozni.

A második minimum az adatkezelés rendbetétele, nem csak papíron! Elméletileg a legtöbb cégnél az érzékeny információk adat-osztályozottak az olyan rendelkezéseknek, szabályozásoknak köszönhetően, mint az uniós AI Act, a GDPR, az ISO-szabványok vagy a NIS2. Legalább odáig el kell jutni, hogy a már osztályozott adatokat megszűrik az AI-jal folytatott „beszélgetésekhez". Nem az a cél, hogy mindent megtiltsunk, hanem hogy legyen egy minimális korlát, ami az alapvető kockázatokat kivédi.

A harmadik minimum, hogy ne bízzunk vakon abban, hogy „majd mindenki észreveszi" a gyanús tartalmakat. Intenzíven ellenőrizni és logolni kell, mindezt olyan módon, hogy szükség esetén auditorok megfelelő jogosultsággal vissza tudják nézni, mi történt. Itt akár maga az AI és részt vehet a védelemben, lehet egy AI-eszközzel keresni vagy modellezni, hogy bizonyos típusú adatok kimentek-e valahova vagy milyen kontextusban kerülhetnek ki.

Az egyéni óvatosság a mai világban már nem működik, ugyanakkor nem hiszek abban, hogy a munkahelyi és emberi környezet alkalmas rá arra, hogy állandóan azonosítgassuk magunkat. Automatizmusokra és működésbe épített keretekre van szükség, úgy, hogy közben használható rendszert adunk a kollégák kezébe, különben mindenki a saját eszközeivel fog megoldást találni.

BIZONYTALANSÁG ÉS KONTROLLVESZTÉS

Mivel jár, ha nehezebb eldönteni, mi a valós?

A generatív AI terjedéséről sokszor a hatékonyság, a gyorsaság és az új lehetőségek kapcsán beszélünk. Ezek a szempontok valósak, ugyanakkor a technológiai fejlődésnek van egy kevésbé látható következménye is.

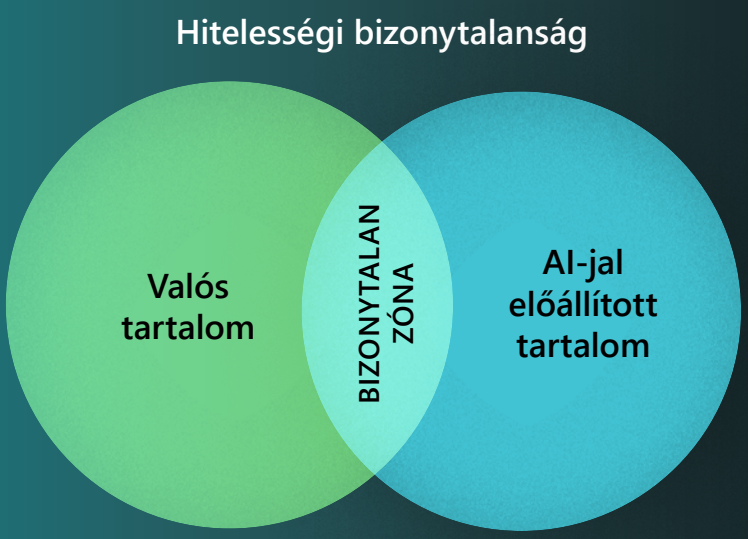
AHOGY A GENERÁLT TARTALMAK EGYRE VALÓSÁGHŰBBÉ VÁLNAK, sok ember számára nehezebb lesz biztosan eldönteni, hogy amit olvas, amit lát, vagy amit hall, az valódi-e. A Microsoft korábban említett kutatása amelyben 15 ország közel 15 000 embert kérdeztek - eredményei szerint csupán egyetlen év alatt 46%-ról 25%-ra esett vissza a deepfake videók felismerési aránya, azaz, ma már csak minden negyedik ember tudja megkülönböztetni a valódi és a mesterségesen manipulált videókat. Az efféle bizonytalanság nemcsak információs kérdés, mivel mentális terhelést, nyugtalanságot eredményezhet, ami megzavarja a kognitív és érzelmi képességeket is.

A mindennapi tájékozódásunk alapja a bizalom. A legtöbb helyzetben nem elemzünk mindent külön, inkább gyorsan döntünk, szelektálunk, és a megszokott jelekre támaszkodunk. Ha azonban ezek a jelek gyengülnek, mert egy szöveg, kép, videó vagy hang sokkal hihetőbbé válik, akkor a döntésekhez több mentális energiára van szükség. A felhasználónak többször kell megállnia, ellenőriznie, mérlegelnie. Ez fárasztó, és hosszabb távon stresszélménnyé is válhat, főként akkor, ha a bizonytalanság állandósul.

A kutatás egyik legfontosabb megállapítása, hogy a hitelesség megítélése már most is sokak számára nehezebbnek tűnik. A válaszadók többsége egyetért azzal az állítással, hogy egyre nehezebb megkülönböztetni, mi valódi, és mit készített AI. Ez a jelzés azért különösen erős, mert nem egy szűk, technológiai érdeklődésű csoport benyomásairól van szó, hanem egy reprezentatív munkavállalói mintáról. A megkülönböztetési bizonytalanság így nemcsak médiatudatossági kérdésként jelenik meg, hanem a hétköznapi biztonságérzetet érintő tapasztalatként is.

A bizonytalanságból többféle mentális reakció következhet. Van, akiben ez fokozott gyanakvást vált ki, amitől

MENTÁLIS HATÁSOK



> „Majdnem mindent kétséggel, gyanakvással fogadunk. Amíg nem bizonyosodunk meg más forrásokból, addig mindent fenntartásokkal kezelünk. Még az AI-generált kódrészleteket is ellenőrizzük tesztkörnyezetben."
>
> Szakértő ESET partner

a tájékozódás nehezebb, lassabb lesz. Másoknál inkább a kontrollvesztés érzése erősödhet, mert úgy élhetik meg, hogy nem tudnak megbízható kapaszkodók alapján dönteni. Megint másoknál a folyamatos készenlét lehet megterhelő, mert minden információ ellenőrizendővé, gyanússá válik. A közös pont az, hogy a hitelesség megítéléséhez megterhelőbb mentális munkát kell végezni és ez reaktív stresszhez, szorongáshoz vezethet, különösen akkor, ha a felhasználó azt érzi, nincs biztos eszköze arra, hogy megbizonyosodjon a tartalmak valódiságáról. A valóság hiperrealisztikus meghamisításának lehetőségére fel kellene készülni, amihez egyelőre nincsenek érzelmi fogódzóink.

A kutatásból az is kitűnik, hogy az AI-hoz fűződő viszony nem egyirányú. A felhasználók egy része lelkesedéssel tekint a technológiára, sokan hasznosnak, hatékonynak látják és szívesen próbálnak ki új eszközöket. Ezzel párhuzamosan azonban megjelenik az aggodalom is, részben a hitelesség bizonytalansága, részben a hosszabb távú társadalmi következmények miatt. Ez a kettősség önmagában is magyarázza, miért fontos az AI-használat mentális dimenziójának feltérképezése. Nem azért, hogy a technológiát veszélyforrásként címkézzük, hanem azért, hogy értsük, milyen feszültségek keletkezhetnek a mindennapi használatban.

Ez a mentális szál közvetlenül kapcsolódik a biztonsághoz is: ha a felhasználó bizonytalan, könnyebben kerülhet nyomás alá és hozhat elhamarkodott döntéseket, főleg akkor, ha az üzenet sürgető, vagy megjelenik benne a tekintéllyel összefüggő nyomás. A whitepaper következő részében ezért a munkahelyi jövőképet és az alkalmazkodás által jelentett nyomást vizsgáljuk meg közelebbről, mert a bizonytalanság nemcsak a tartalmak hitelességére, hanem a munka világának átalakulására is kiterjedhet.

SZAKÉRTŐI KOMMENTÁR

TARI ANNAMÁRIA

Miért szorongáskeltő, ha csökken a kontrollélmény, hogyan hat a tartós bizonytalanság a döntésekre, és mi segíthet a mindennapi megküzdésben.

Az internet látszólag korlátlan szabadságot nyújt számunkra, azonban a végtelen információs halmaznak csak töredéke jut el hozzánk. A háttérben futó algoritmusok miatt véleménybuborékba kerülünk, amelybe az érdeklődésünkkel vagy véleményünkkel ellentétes tartalmak nem kerülnek be. Így már most is irányított érdeklődési körünk van, amit a sajátunknak érzünk.

Ennek a kezelésére önreflexióra lenne nagy szükség, ez lehet a pajzs, ami megvéd nehéz érzelmi helyzetekben. Ha a munkavállalóknak fel kell készülnie egy olyan helyzetre, ahol munkája kiváltható, vagy nem fejlődik megfelelően, akkor az újratervezési képességét, megküzdő stratégiáit kell fejlesztenie. Ellenkező esetben megnő a veszélye a „tanult tehetetlenségnek", amikor azt éli át, hogy semmit sem tud elérni.

A kontrollvesztés élménye az egyik legijesztőbb állapot, amelynek enyhébb változatait régóta gyakoroljuk, amikor engedelmeskedünk az algoritmusnak.
Az érzelmi és mentális stabilitást ebben a helyzetben is a személyiség érzelmi egyensúlya adja, amihez stabil külső környezet is kell.

Munkahelyek jövője, alkalmazkodási nyomás, ambivalencia

Az AI terjedésével kapcsolatos aggodalmak terén az egyik leggyakoribb félelem a munka világával kapcsolatos. Ez a téma ugyanis nem elvont technológiai kérdésként jelenik meg, hanem a saját feladatokra, a munkahelyi elvárásokra, a fejlődési kényszerre és hosszabb távon a munkahelyek sorsára vonatkozó bizonytalanságként.

KUTATÁS ALAPJÁN EZ A TÉMA ERŐSEN JELEN VAN A MUNKAVÁLLALÓI GONDOLKODÁSBAN, ami könnyen válhat feszültségforrássá, mert egyszerre kapcsolódik a megélhetéshez, az identitásunkhoz és a biztonságérzethez.

A válaszadók jelentős része egyetért azzal az állítással, hogy az AI terjedése miatt bizonyos állások veszélybe kerülhetnek, és sokan gondolják azt is, hogy egyes feladatoknál már nem lesz szükség emberre. Ezek a vélekedések nem feltétlenül személyes jóslatok, inkább társadalmi várakozások, amihez hozzájárulhattak az elmúlt években gyakran megjelenő, a témával foglalkozó cikkek, híradások. Ezek mentális hatása ugyanakkor ettől még teljesen valós, mert a bizonytalanság önmagában is megterhelő. Ha valaki úgy érzi, hogy a munka világa gyorsan változik, és nem világos, hol lesz a helye ebben a változásban, az szorongást, feszültséget és egyfajta fokozott készenléti állapotot idézhet elő.

A munkahelyi aggodalom azonban nem csak az állások megszűnésének félelméről szól. Legalább ilyen erősen megjelenhet a lemaradástól való félelem és a kompetenciával kapcsolatos szorongás. Sokan érzik úgy, hogy aki nem tudja használni az AI-t, az hátrányba kerülhet a munkahelyén. Ez a gondolat nem feltétlenül konkrét fenyegetésként jelenik meg, inkább úgy, mint folyamatos alkalmazkodási kényszer. A felhasználók egy része úgy élheti meg, hogy miközben új készségeket kell megtanulni és lépést kell tartani, közben nem mindig világos, mi számít elég tudásnak, vagy mihez képest maradnak le. Ez a bizonytalanság könnyen krónikus stresszhelyzetet teremt, különösen akkor, ha a munkahelyi elvárások nincsenek kimondva és a támogatás sem egyértelmű.

MENTÁLIS HATÁSOK

A kutatásban ugyanakkor erősen jelen van a lehetőségek oldala is. Sokan gondolják úgy, hogy az AI segíthet hatékonyabban dolgozni, így több idő maradhat a kreatívabb, értékesebb feladatokra. A nyitottság is megjelenik: sokan szívesen kipróbálnak új eszközöket és a mindennapi használat során is látják a tényleges hasznot, amit a technológia adhat. Fontos azonban egyszerre értelmezni a helyzet kettősségét. A lehetőségek és az aggodalmak nem egymást kioltó tényezők, hanem ugyanannak a jelenségnek a két oldalát képviselik. Sok esetben ezek egyszerre vannak jelen a társadalom hangulatában, de akár ugyanazon embereknél is. Valaki lehet egyszerre kíváncsi és óvatos, egyszerre lelkes a hatékonyság miatt, és közben bizonytalan a hosszabb távú következmények miatt.

A mentális terhelés akkor erősödik, amikor több bizonytalansági forrás összeadódik. A korábban bemutatott hitelességi bizonytalanság, a munka világának átalakulásával kapcsolatos várakozások és a lemaradási nyomás együtt olyan környezetet teremthet, ahol a felhasználók tartósan "érzelmi készenléti állapotba" kerülnek. Ilyenkor a döntések fárasztóbbá válnak, és a stressz szintje is emelkedhet. A kutatásban a stressz, szorongás és kockázatérzet témái ezért nem különálló, hanem egymással összefüggő jelenségek.

58 százalék szerint hátrányba kerülhet, aki nem tudja használni az AI-t

Kiemelt kutatási statisztika

A következő részben a mentális hatást kötjük össze az IT-biztonsági nézőpontokkal. A bizonytalanság és a stressz ugyanis nem csak belső élmény, hanem hatással lehet arra is, mennyire tudunk kritikusak maradni, mennyire állunk meg ellenőrizni, és mennyire vagyunk megtéveszthetők akkor, amikor sürgető vagy tekintélyhelyzetet sugalló megkeresésekkel találkozunk.

SZAKÉRTŐI KOMMENTÁR

TARI ANNAMÁRIA

A kritikai gondolkodás és AI-tudatosság kérdéséhez szorosan kapcsolódnak a kognitív képességeink: gondolkodás, figyelem, kontextusok értelmezése. A források ellenőrzésének, illetve a hallucinációk kivédésének rutinná kell válnia az AI-használat során, ez hosszabb időt vesz igénybe. Ameddig ezen tudás formálódik, számolni kell a visszatérően jelentkező stressz érzéseivel, és a kompetenciaszorongással, amely a saját értékek, a szakmai tudás és a kognitív képességek fenntartásának lehetetlenségével vagy csökkenésével fenyeget.

A modern vezetőnek képesnek kell lennie rá, hogy elkerülje a tudás illúzióját és a Dunning-Kruger hatást.

Kutatások kimutatták, hogy a mesterséges intelligenciába vetett bizalom kevesebb kritikai gondolkodással, a nagyobb önbizalom a kritikusabb gondolkodással jár. Az alacsonyabb szakmai önbizalom viszont gátolhatja a kritikai gondolkodást, növelve az AI felé érzett elköteleződést, ami hosszú távú függőséghez és a problémamegoldási készség csökkenéséhez vezethet.

Ez az eredmény azt mutatja, hogy a jövőben a biztos és alapos szakmai tudás lesz a bázisa az önálló gondolkodásnak, a kreatív ötleteknek. Ha engedünk annak a vágyvezérelt gondolkodásnak, hogy az AI mindent tud és mindenre képes, akkor olyan alárendelődő szerepbe kerülünk, ahol a döntési bizonytalanság erősödni fog.

A BIZONYTALANSÁG IT-BIZTONSÁGI ÁRA

A stressz növeli a megtévesztés esélyét

Az IT-biztonsági kockázatokat gyakran technológiai oldalról értelmezzük, sebezhetőségekről, támadási módszerekről és védelmi megoldásokról beszélünk. A gyakorlatban azonban sok incidens ott kezdődik, ahol egy embernek gyors döntést kell hoznia egy bizonytalan helyzetben.

A BIZALOM EZÉRT NEM ELVONT FOGALOM, hanem a mindennapi döntéseknél észlelhető rizikófaktor. Ha a felhasználó bizonytalan abban, hogy egy üzenet vagy hívás hiteles-e, miközben sürgetik is, akkor könnyebben tévedhet, és könnyebben válik befolyásolhatóvá.

A döntési helyzetek logikája viszonylag egyszerű, ahogy azt akár a hétköznapok során is tapasztalhatjuk. Ha túl sok információ érkezik egyszerre, nő a kognitív terhelés, aminek eredményeként kevesebb időt, illetve energiát fordítunk arra, hogy minden részletet végiggondoljunk. Ha időnyomás alá kerülünk, nagyobb eséllyel reagálunk azonnal, ellenőrzés nélkül. Ha pedig az adott helyzetben megjelenik a tekintély kérdése, például egy felettes, vezető vagy hivatalos(nak tűnő) személy, akkor könnyebben beadjuk a derekunkat és gyorsabban teljesítjük a kérést. Ezek a reakciók önmagukban nem hibák, hanem emberi mintázatok. Biztonsági kockázattá akkor válnak, amikor a megtévesztő tartalom valósághű, a sürgető helyzet pedig a felhasználót a gyors cselekvés és a feszültségtől való megszabadulás felé tolja.

A kutatás adatai azt jelzik, hogy több olyan tényező is egyszerre van jelen, amely növelheti ezt a kockázatot. A válaszadók többsége úgy érzi, hogy egyre nehezebb megkülönböztetni, mi valódi, és mit készített AI. Sokak szerint az emberek túlságosan megbíznak abban, amit az AI javasol, és nem elég óvatosak akkor sem, amikor információkat osztanak meg AI-jal. Ezek a megállapítások együtt azt rajzolják ki, hogy a mindennapi biztonság egyre inkább a hitelesség megítélésén, az ellenőrzési rutinokon és az információkezelési szokásokon múlik.

Ezen a ponton fontos megtartani a megfelelő egyensúlyt, mert a két szélsőség egyaránt kockázatos. A hamis biztonságérzet, amikor mindent elhiszünk és nem ellenőrzünk, könnyen vezet hibához. A teljes bizalmatlanság, amikor semmit nem fogadunk el hitelesnek, szintén problémát

MENTÁLIS HATÁSOK

SZAKÉRTŐI KOMMENTÁR **CSIZMAZIA-DARAB ISTVÁN**

Hogyan jelenik meg a mentális állapot és a stressz kérdése a mindennapi támadási helyzetekben, és mi a minimális ellenőrzési lépés, amit érdemes beépíteni?

Érdekes jelenség a tudatos használat hiánya mellett, hogy sokan akkor is AI-jal generáltatnak valamilyen munkajellegű anyagot, ha egyébként ők maguk jobban meg tudnák csinálni, pedig a saját anyagaikat véleményeztethetnék, javíthatnák is vele. Ez hosszú távon rossz hatással lehet az önértékelésükre.

A digitális tájékozatlanság közvetlenül is növeli az áldozattá válás lehetőségét, de például az érzelmi manipulációra építő tartalmak által kiváltott düh vagy ijedtség is gyakran hibázáshoz vezethet. Ilyenkor a célpont nem viselkedik kellő óvatossággal, aminek következménye lehet, hogy beleesnek a támadók csapdájába.

A biztonsági minimum, amit minden cégnél be kellene vezetni, magában foglalja az alapvető irányelveket, azaz, hogy mit szabad és mit nem (BYOD, shadow IT, shadow AI), a rendszeres biztonságtudatossági képzéseket és teszteket, az ismeretanyagok frissítését, az incidensek jelentésének szigorú protokollját, valamint a jóváhagyott eszközök és adatkezelési elvek körét és mindezek következetes betartatását.

okoz, mert lelassítja a működést, rombolja a jóhiszemű kommunikációt, és hosszabb távon fokozhatja a szorongást is. A cél nem az, hogy a felhasználók állandó gyanúban éljenek, hanem az, hogy legyenek olyan egyszerű, ismételhető lépések, amelyek csökkentik a hibázás esélyét, különösen sürgető vagy tekintélyt sugalló helyzetekben.

A szervezeti keretek itt kézzel foghatóan segíthetnek. Ha van bevett gyakorlat a visszaellenőrzésre, például egy másik csatornán történő megerősítésre, akkor a felhasználónak nem egyedül kell eldöntenie, mi hiteles. Ha a pénzügyi, hozzáférési vagy adatkiadással járó kérésekhez egyértelmű jóváhagyási rend tartozik, akkor a sürgetés kevésbé tud célt érni. Ha pedig létezik egyszerű jelzési útvonal, ahova gyanús megkereséseket tovább lehet küldeni, az csökkenti az egyéni bizonytalanságot, és gyorsítja a szervezet tanulását is. Ezek az intézkedések nemcsak biztonsági szempontból fontosak, hanem mentális oldalról is, mert csökkenthetik a kontrollvesztés élményét.

A whitepaper következő részében összefoglaljuk, hogyan kapcsolódik össze a három vizsgált terület. A használat tömegesedése, az IT-biztonsági kockázatok és a mentális terhelés nem különálló jelenségek, hanem ugyanannak a változásnak az eltérő nézőpontjai.

Hogyan ér össze a használat, a kockázat és a mentális terhelés?

A kutatás alapján a generatív mesterséges intelligencia mára a magyar munkavállalók mindennapjainak része lett. A használat gyorsan terjed, gyakran egyéni rutinok mentén, miközben a munkahelyi keretek sok esetben csak késve alakulnak ki.

EZ EGYSZERRE JELENT ÚJ LEHETŐSÉGEKET, és egyszerre hoz olyan helyzeteket, amelyek kockázati tényezővé válhatnak, ha nincs közös iránytű, nincs ellenőrzési gyakorlat, és nincs világos felelősség.

A legfontosabb tanulság, hogy az AI ma már nem egy szűk, technológiában jártas réteg ügye. A munkavállalók jelentős része találkozott vele, a belépési pont pedig jellemzően néhány jól ismert AI-eszköz. Ez a koncentráció azt eredményezi, hogy a felhasználói szokások gyorsan tömegesednek, és a mindennapi feladatokban is megjelennek. A használat fókusza pedig elsősorban a tájékozódáson, az információgyűjtésen

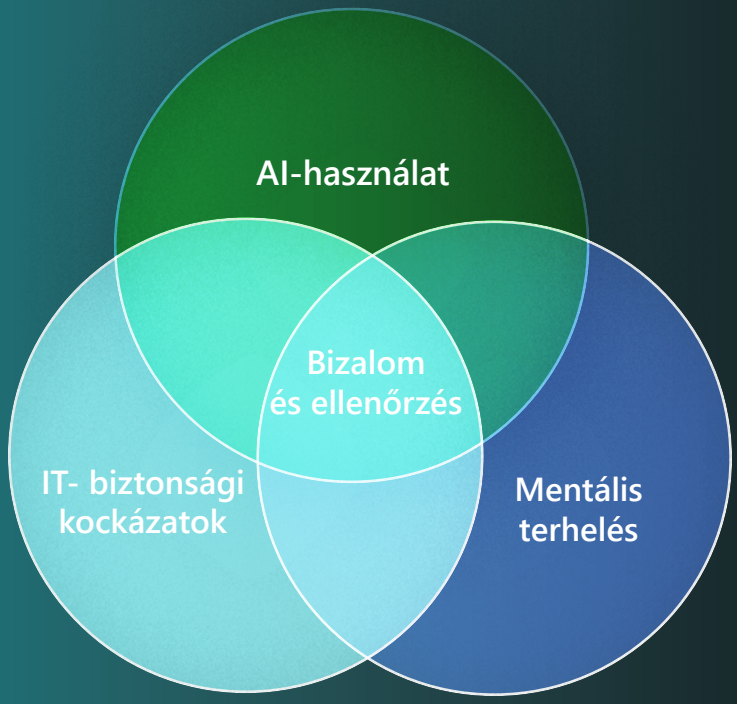
ÖSSZEGZÉS

és a szövegalapú feladatokon van, vagyis ott, ahol döntések és munkafolyamatok előkészítése történik.

A munkahelyi oldalon közben az látszik, hogy a használat sokszor megelőzi a szervezeti felkészülést. A kutatás szerint sok munkahelyen nincs hivatalos párbeszéd arról, mire és hogyan érdemes AI-t használni, illetve a továbbképzések kérdése sem tisztázott még sok helyen. Ilyenkor a jó gyakorlatok nem egységesek a munkavállalók pedig gyakran saját megérzésekre, informális tanácsokra, vagy egyszerű kényelmi döntésekre támaszkodnak. Ez nem rosszindulat kérdése, hanem egy természetes átmeneti állapot, amely azonban kockázatokkal jár.

Az ilyen rizikófaktorok közül több a bizalom és ellenőrzés köré szerveződik. A felhasználók túlnyomó többsége fontosnak tartja, hogy az AI eredményeit ember is ellenőrizze, mégis sokak szerint az emberek hajlamosak túl sokat elhinni abból, amit az AI javasol. Ugyanígy jellemző vélekedés, hogy az információk megosztásánál is gyakran hiányzik a kellő körültekintés. Ezek a jelzések arra utalnak, hogy a kockázat nem csak technikai, hanem döntési és viselkedési kérdés is.

A kutatás egyik legfontosabb sajátossága, hogy a mentális hatásokat is célzottan vizsgálja, különösen a hitelesség megítélésének kérdését. A válaszadók többsége úgy érzi, egyre nehezebb megkülönböztetni, mi a valódi, és mit készített AI. A valósághű generált tartalmak terjedése ezért nem csak információs kihívás, hanem mentális teher is lehet. A bizonytalanság tartós élménye stresszt, szorongást és a kontrollvesztés érzését okozhatja, ezzel párhuzamosan növelve a megtévesztés kockázatát is, mert a támadók kifejezetten az AI-generált tartalmak látszólagos hitelességére építenek.



A fenti tanulságok közös pontja, hogy a biztonságos AI-használat nem elsősorban egyéni ügyesség kérdése. Szervezeti szinten kell megteremteni a célokat, a használati kereteket, az adatkezelési alapelveket, az ellenőrzési és hitelesítési rutinokat, valamint a képzési hátteret és a felelősségi rendet. Ezek az elemek egyszerre csökkenthetik az IT-biztonsági kockázatokat, és a bizonytalanságot, mert a felhasználók nem maradnak magukra a döntéseikkel.

A technológiai fejlődés gyors, ezért a felkészülés nem halogatható. A whitepaper célja, hogy a magyar munkavállalói valóságból kiindulva, adatokra támaszkodva mutassa meg, hol vannak a legfontosabb csomópontok, és miért fontos a használat, a biztonság és a mentális terhelés kérdéseit együtt kezelni.

ellenőrzés

hitelesítés

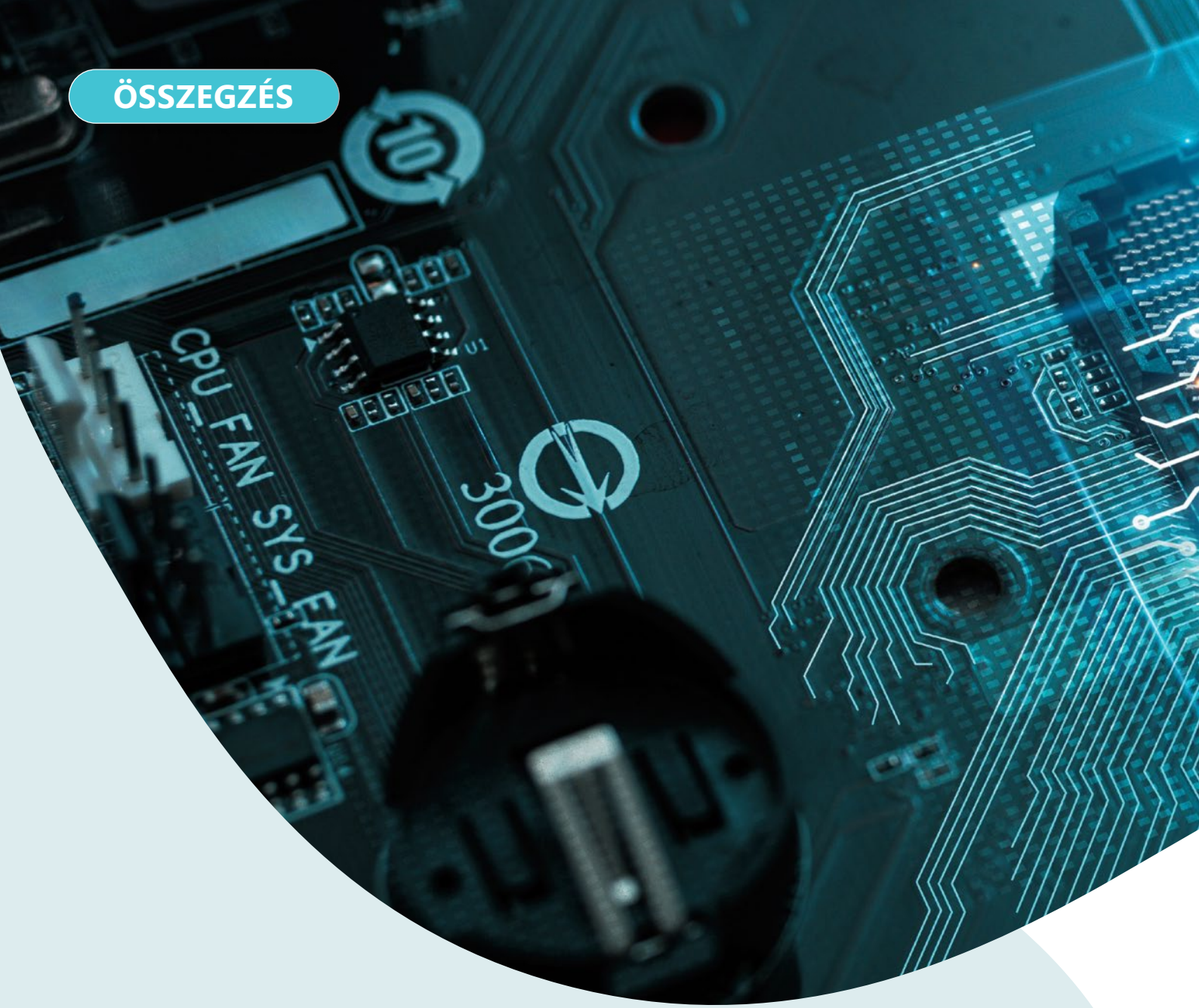
Hogyan őrizhető meg a bizalom a valósághű tartalmak korában?

A generatív AI ma már nem csupán egy új eszköz, hanem egy olyan paradigmaváltás, amely egyre több munkafolyamatban jelenik meg. Sok szervezetben már nem az a kérdés, hogy használják-e, hanem az, hogy milyen módon épül be a mindennapi működésbe.

A **HASZNÁLAT GYORS ÜTEMŰ TERJEDÉSE,** illetve a technológia széleskörű és mélyrenyúló hatásai miatt pedig a keretek és rutinok nem átmeneti kérdések. A most kialakított keretek hosszú távon velünk maradnak és meghatározzák, hogy a technológia inkább segítség lesz, vagy kockázati tényezők forrása.

A whitepaper egyik legfontosabb nyitott kérdése ezért számunkra az, hogy mi történik akkor, ha az AI használata idővel elvárássá válik. Hogyan alakul a felelősség, mi számít jó gyakorlatnak, és ki viseli a következményeket, ha hiba történik? Hogyan marad meg a döntések emberi kontrollja olyan helyzetekben, amikor az AI egyre

ÖSSZEGZÉS



„A mesterséges intelligencia és különösen az AI-ügynökök megjelenése átalakítja az azonosítás és a hitelesség igazolásának folyamatait. Olyan AI-alapú megközelítések jönnek, amelyek a helyzetet és a felhasználói szándékot is értelmezik. A felkészülés lényege ezért nem az, hogy megállítsuk ezt, hanem hogy kialakítsuk azokat az új normákat és működési kereteket, amelyekben a döntések következménye továbbra is emberi felelősség marad, miközben a mindennapi működés biztonsági kontrolljának egyre nagyobb része automatizált, kontextusérzékeny rendszerekbe épül. Ezen felül szükséges lesz minden munkavállalónak belátnia, hogy egyfajta AI munkatársak csoportvezetőjeként és kreatív feladatszervezőként kell működnie."

KELETI ARTHUR

több ponton ad javaslatot, fogalmaz meg szöveget, vagy készít elő döntést? Ezekre a kérdésekre nincs egyetlen, egyszerű válasz, viszont a tétjük világos. A szervezeteknek úgy kell kialakítani a saját működésüket, hogy közben megőrizzék a munkavállalóik és ügyfeleik felé a bizalmat, a biztonságot és a kiszámíthatóságot.

A kutatás alapján különösen fontos a bizalom és az ellenőrzés viszonyát újragondolni. A valósághű tartalmak korában a hitelesség megítélése nehezebb, ezért a hitelesítés nem épülhet kizárólag egyéni megérzésekre. A visszaellenőrzésnek, a jóváhagyási rendnek és a több csatornás megerősítésnek a munka természetes részévé, rutinná kell válnia. A szervezeti keretek ebben a megközelítésben nem tiltások, hanem támpontok, amelyeknek az a célja, hogy a felhasználók pontosan tudják, mi fér bele, mihez kell ellenőrzés, és mikor kell megállni.

A mentális dimenziót is érdemes komolyan venni. A bizonytalanság, amely abból fakad, hogy nehezebb eldönteni, mi hiteles, sokaknál stresszt és a kontrollvesztés érzését okozhatja. Ugyanez igaz az alkal-

Az emberi idegrendszer és érzelmi apparátus csak látszólag alkalmazkodik könnyen. A nem emberi rendszerek lényegének el- és befogadása nem csak kognitív képességeken múlik. Az AI mellé rendelhető érzelmek egyelőre inkább stressz-, és szorongásalapúak, akkor is, ha egyébként a felszínen azt hisszük, mi kormányozzuk ezt a hajót. Emberi szituációkból alkotunk egyelőre hipotéziseket, amelyeknél látványosan elkülönül a felhasználók pozitivitása és a többiek dilemmája. Minden elvárás, amit úgy írunk le, mint szinte kötelező érzelmi attitűdöt, egy eddig sosem megélt helyzetben jóval lassabban alakulhat csak. Évekkel korábban már láttuk, hogy amennyire kifárasztja az idegrendszert ha elárasztják az impulzusok, ez most a kontroll elvesztésének félelmével kiegészülve komoly mentális teherré válhat. A megoldás a reális és optimális önbizalom és szakmai tudás kialakítása.

TARI ANNAMÁRIA

ÖSSZEGZÉS

"Vállalati környezetben az MI nem játszótárs, hanem nagy teljesítményű eszköz, ahol a hibázásnak vagy az adatszivárgásnak valódi ára lehet. Mivel az AI-rendszerekbe vitt adatok felett a küldés után megszűnik a kontroll, elengedhetetlen a szigorú szervezeti szabályozás és az érzékeny információk manuális előszűrése.A belső szabályozásnak ki kell térnie a szerepkör alapú hozzáférésre, az engedélyezett eszközök meghatározására, a használat során az érzékeny adatok maszkolására, anonimizálására, valamint az MI által végzett eredmények mindenkori emberi ellenőrzésére."

CSIZMAZIA-DARAB ISTVÁN

mazkodási nyomásra is, amikor a munkavállalók úgy érzik, folyamatosan lépést kell tartaniuk. A tiszta keretek és a kiszámítható rutinok nemcsak a biztonsági kockázatot csökkentik, hanem a mentális terhelést is mérsékelhetik. Ha a felhasználók nem maradnak egyedül a döntéseikkel és vannak megfelelő kapaszkodóik, akkor a bizonytalanság kezelhetőbbé válik.

A minőségi IT-biztonsági megoldások hatékony védelmet nyújtanak sokféle, a fentiekben tárgyalt kockázattal, veszéllyel szemben. Megakadályozzák a zsarolóvírusok futtatását, letiltják az adathalász oldalakat, kiszűrik a káros csatolmányokat. Azonban, az IT-biztonságnak akadnak olyan területei, amelyeket jellegükből adódóan nem tudnak lefedni. Ilyen például az, amikor érzékeny céges adatokat dolgoznak fel a munkatársak a saját, ingyenes AI-fiókjukkal. Ez egy szürke, de inkább sötét zóna, amelynek kockázataival kapcsolatban az ESET - felelős vállalatként - szeretné felhívni a szakemberek, de a felhasználók figyelmét is.

Ez a whitepaper azért készült, hogy a témáról hiteles adatok alapján beszéljünk, illetve közös nyelvet alakítsunk ki a szervezetekkel, a munkavállalókkal és a nyilvánossággal. A technológiai fejlődés gyors, de a felkészülés nem lehet egyszeri projekt. Folyamatos tanulásra, fejlődésre van szükség, amely során a használati szokások, a biztonsági kockázatok és a mentális hatások együtt alakítják ki azt, amit a jövőben biztonságos, felelős AI-használatnak nevezünk.

„Az AI fejlődésével egyre közelebb kerül az átlagos felhasználókhoz, az egyre alacsonyabb belépési küszöb miatt pedig nem akkor fognak sokan hátrányba kerülni, ha nincsenek megfelelő technológiai ismereteik, hanem akkor, ha nem tanulnak meg kritikusan kérdezni és tényeket ellenőrizni. A tudatos használat lényege, hogy a hasznosságot nem keverjük össze a hitelességgel. Az AI gyorsít és támogat, de az ellenőrzés felelőssége végig a mi oldalunkon marad."

KEREK ISTVÁN

Források jegyzéke

Vezetői köszöntő

- Sicontact Kft. – Az ESET magyarországi hivatalos forgalmazója (kutatási megbízó)

Bevezető

- Microsoft: Global Online Safety Survey (2026. február 10.)
- Digital Safety | Global Online Safety Survey Results (Microsoft weboldal)

AI-alapok I.

- Az ESET számára készült reprezentatív kutatás (reprezentatív kutatás a magyar társadalomban, 2026 eleje)
- Általános körkép az AI helyzetéről II. – Technológiai háttér
- RunwayML: Runway Research: The Turing Reel (2026. január 22.)
- Prizma Alapítvány és az Europion: „Már a szemünknek sem hiszünk" közös kutatás (2026. február)
- Az ESET számára készült nagymintás kutatás (AI-tudatosság elemzés és kérdőíves eredmények összefoglalója, N=600)
- Kutatási ismertető: módszertan, minta, értelmezési keretek
- Medián Közvélemény- és Piackutató Intézet (adatfelvétel: 2025. november 25–28.)
- Sicontact Kft. (kutatási megbízó)

AI-használat I.

- Az ESET számára készült nagymintás kutatás (AI-tudatosság elemzés és vezetői összefoglaló)

AI-használat II.

- Az ESET számára készült nagymintás kutatás (felhasználási célok, elégedettségi megoszlás és demográfiai mintázatok)

AI-használat III.

- Az ESET számára készült nagymintás kutatás (munkahelyi kommunikáció, képzés és segítségkérés arányai)

IT-biztonság I.

- Az ESET számára készült nagymintás kutatás (Likert-skálás attitűd-állítások az ellenőrzésről, bizalomról és adatmegosztásról)

IT-biztonság II.

- Az ESET számára készült nagymintás kutatás (AI-tudatosság elemzés és Sicontact kérdőív eredményösszefoglaló)

IT-biztonság III.

- Az ESET számára készült nagymintás kutatás

Mentális hatások I.

- Microsoft: Global Online Safety Survey 2026
- Az ESET számára készült nagymintás kutatás (hitelesség megítélése és attitűdök)

Mentális hatások II.

- Hao-Ping (Hank) Lee et al.: The Impact of Generative AI on Critical Thinking (CHI '25 Conference, 2025)
- Az ESET számára készült nagymintás kutatás (lemaradási nyomás és munkahelyi jövőkép)

Mentális hatások III.

- Az ESET számára készült nagymintás kutatás (bizalom és kockázatérzékelés)
- VISA-kutatás (érzelmi manipuláció és digitális tájékozatlanság kapcsán)

Összegzés I. és II.

- Az ESET számára készült nagymintás kutatás (összesített eredmények és vezetői összefoglaló)

SICONTACT
biztonság a digitális világban

E-mail: biztonsag@sicontact.hu
Telefon +36 (1) 346 7052