A digitális kockázatok 2026-ban

Részletes magyar összefoglaló az áttekintésről, a fő kockázatok elemzéséről, a szervezeti válaszokról és az előretekintésről. A feldolgozott anyag a Digital Risk Report 2026.

A digitális kockázati térkép

A jelentés a 2026-os digitális környezetet gyors technológiai fejlődés, széttagolódó szabályozás és fokozódó geopolitikai feszültség metszéspontjaként írja le. A generatív és ügynöki mesterséges intelligencia már nem pusztán kísérleti eszköz. Egyre több üzleti folyamatba épül be, adatokat dolgoz fel, döntéseket támogat vagy hajt végre, és közvetlen kapcsolatba kerül ügyfelekkel. Ezzel párhuzamosan a szervezeteknek eltérő nemzeti szabályoknak, kiberfenyegetéseknek és belső működési hiányosságoknak kell megfelelniük.

A kockázatkezelés ezért stratégiai szerepet kap. A cél egyszerre a károk megelőzése és annak megteremtése, hogy a szervezet megfelelő kontrollok mellett merjen új technológiát alkalmazni. A jelentésben bemutatott felmérésben közel 600 digitális kormányzási szakember választotta ki a 23 kockázat közül a három legfontosabbat. A kockázatok négy csoportba rendeződnek: geopolitikai, szervezeti, technológiai, valamint társadalmi és környezeti tényezők.

81%	77%	5 / 10
legalább egy geopolitikai kockázatot a három legfontosabb közé sorolt	legalább egy szervezeti kockázatot jelölt a három legfontosabb között	a tíz legfontosabb kockázat közül geopolitikai jellegű

Külső nyomás és belső sérülékenység

A válaszadók közel 40%-a az egymásnak ellentmondó nemzeti követelményeket nevezte a kiszámítható adatvédelmi környezet fő jogi akadályának. A szervezetek gyakran a legszigorúbb előírást próbálják minden piacra kiterjeszteni, de ez költséges lehet, és lassíthatja az innovációt a rugalmasabb szabályozású versenytársakhoz képest. Közben a régi folyamatokra épülő új technológia, az elavult adatleltár, a beszállítók felügyeletének hiánya és a kevés szakember egymás hatását erősíti.

Az elemzés az MI káros kimeneteit és szellemi tulajdoni kockázatait, a változó kiberfenyegetéseket, a szabályozási széttagoltságot, a digitális szuverenitást, a beszállítói függést, az irányítási modelleket, a szakember- és költségvetési hiányt, az innováció elmaradását, valamint az MI-befektetések szükségességét vizsgálja.

MI-kockázatok és szellemi tulajdon

Kedvezőtlen kimenetek, torzítás és magyarázhatóság

A megkérdezettek 23%-a az MI kedvezőtlen kimeneteit a három fő kockázata közé sorolta. A modellhibák és az elfogult eredmények egészségügyi, pénzügyi vagy stratégiai döntéseket befolyásolhatnak. A kockázat különösen súlyos ott, ahol egy hibás ajánlás közvetlenül érinti a betegbiztonságot, a hitelezési döntést vagy az ügyfélnek nyújtott szolgáltatást. A nem megfelelő, hiányos vagy nem reprezentatív tanítóadat hibás eredményhez vezethet, az elfogultság pedig jogi felelősséget és bizalomvesztést okozhat.

A modellek összetettsége miatt a szervezetek gyakran nem tudják könnyen megmagyarázni, hogy egy adott eredmény miért született. Ez megnehezíti a teljesítmény ellenőrzését, a hiba okának feltárását, az elfogultság csökkentését és annak bizonyítását, hogy a döntés megfelel az ágazati vagy adatvédelmi követelményeknek. A magas kockázatú rendszerekre vonatkozó szabályok ezért dokumentálást, magyarázhatóságot és felelős emberi felügyeletet várnak el.

Ügynöki MI és tovagyűrűző hibák

Az autonóm MI-ügynökök egymással, vállalati rendszerekkel és külső szolgáltatásokkal is kapcsolatba léphetnek. Ha céljaik, jogosultságaik vagy utasításaik ütköznek, hibás vagy nem szándékolt műveleteket hajthatnak végre. Egy kisebb tévedés több rendszerre átterjedhet, automatizált folyamatokat indíthat el, vagy ügyfélkapcsolatokat és pénzügyi döntéseket érinthet. A kockázat nem kizárólag az egyes modellekből, hanem az összekapcsolt működésből is ered.

Az ügynöki kereskedelemben az MI a fogyasztó nevében kereshet, tárgyalhat és vásárolhat. A közvetlen szabályozási útmutatás és a felelősségi határok még kialakulóban vannak. A megbízható tokenek és a súrlódásmentes vásárlási folyamatok a csalásfelderítést is nehezíthetik, miközben a támadók automatizálhatják a jogosulatlan tranzakciók kipróbálását.

MI és szellemi tulajdon

A generatív MI fejlesztése és alkalmazása szerzői jogi, védjegy-, üzleti titok- és egyéb szellemitulajdon-jogi vitákhoz vezethet. A szervezet saját vagy ügyfelei adatait is kiteheti jogosulatlan felhasználásnak, ha nem ismeri pontosan a modell adatkezelési gyakorlatát. A kimenetek eredete és az egyes tartalmak forrása nehezen követhető, ezért a jogsértés felismerése és bizonyítása is bonyolult.

A vállalatoknak egyszerre kell védeniük saját innovációjukat, szerződéses jogaikat és üzleti modelljüket, valamint felkészülniük a harmadik felek igényeire. A szabályozás és a bírósági gyakorlat változása üzleti bizonytalanságot okoz, különösen a tartalom-, szórakoztató- és technológiai szektorban. A beszerzési feltételek, az adatok eredetének nyilvántartása és a modellhasználat szabályozása ezért az irányítás részévé válik.

Változó kiberfenyegetések

Geopolitikai és nemzetbiztonsági összefonódás

A kiberbiztonság régóta ismert kockázati terület, de a gyors digitalizáció elmosta a vállalati informatikai és a nemzetbiztonsági kockázatok közötti határt. A válaszadók 85%-a legalább közepesen magabiztosnak érezte szervezetét a kiberbiztonsági megfelelés terén, miközben az állami szereplőkhöz köthető fenyegetések a Digitális Kockázati Index negyedik helyére kerültek. Az energia- és távközlési infrastruktúrában a kitettség még jelentősebb.

A támadások célja lehet szellemi tulajdon ellopása, a belső infrastruktúra feltérképezése későbbi műveletekhez, a globális ellátási láncok megzavarása, kritikus infrastruktúra destabilizálása, zsarolóvírusos támadás vagy szolgáltatásmegtagadás. A geopolitikai versengésben a szervezetek digitális rendszerei a konfliktusok célpontjaivá vagy közvetett eszközeivé válhatnak. A kockázati helyzet ezért országonként, ágazatonként és szolgáltatói lánconként eltérő.

A mesterséges intelligencia kettős hatása

Az MI gyorsabban azonosíthat sérülékenységeket és segíthet a javításukban. Ugyanezek az eszközök azonban a támadók kezében is felgyorsítják a hibakeresést, a javítások visszafejtését, a változó kódú kártevők létrehozását és a célzott megtévesztő kampányokat. A korábban hónapokig vagy évekig rejtve maradó hibák nagyobb léptékben tárhatók fel. Az MI csökkenti a technikai belépési küszöböt, így támadási képességhez kevésbé tapasztalt szereplők is hozzájuthatnak.

A jelentés példaként olyan fejlett modelleket említ, amelyek képesek lehetnek ismeretlen sérülékenységek önálló kihasználására. A támadási folyamat részleges automatizálása növeli a támadások gyakoriságát, sebességét és célzottságát. A fenyegetést kibővíti, hogy a rosszindulatú eszközök mellett autonóm vagy nem szándékoltan működő rendszerek is okozhatnak incidenst.

Shadow AI és adatbiztonság

Az alkalmazottak által engedély nélkül használt MI-eszközök érzékeny adatot, üzleti titkot, forráskódot vagy ügyfél-információt juttathatnak olyan szolgáltatókhoz, amelyek adatkezelési feltételei nem átláthatók a szervezet számára. A tiltás önmagában gyakran nem oldja meg a problémát, mert a dolgozók továbbra is használhatnak nem jóváhagyott eszközöket. A felügyelet, az elfogadható használati szabályok, az adatbesorolás és a biztonságos alternatívák együtt csökkenthetik a kitettséget.

A kibervédelem feladata egyre inkább a vállalati rendszerek, a beszállítók, az MI-eszközök és a geopolitikai környezet együttes figyelése. Az incidenskezelési és üzletmenet-folytonossági terveknek számolniuk kell azzal, hogy a támadás beszállítói rendszeren keresztül érkezik vagy több szolgáltatást egyszerre érint.

Szabályozási töredezettség, szuverenitás és beszállítók

Szabályozási összetettség és fragmentáció

A digitális szabályozási környezetet a változékonyság, a követelmények nagy száma és a joghatóságok közötti eltérések határozzák meg. Egy multinacionális vállalat egyik piacon alkalmazott megfelelési megoldása egy másik országban ütközhet helyi előírásokkal. Az EU, az Egyesült Királyság, az Egyesült Államok és a feltörekvő szabályozási rendszerek eltérő határidőket, fogalmakat, felelősségi szabályokat vagy átláthatósági követelményeket állapíthatnak meg.

A kisebb szervezetek aránytalanul nagy terhet viselnek. A töredezett szabályozást az összes válaszadó 22%-a nevezte a három legfontosabb kockázat egyikének, a 10 millió dollár alatti bevételű szervezeteknél 35%, az 50 fő alattiaknál 40% volt ez az arány. A szervezetnek mérlegelnie kell a jövőbeli szabályokra való előzetes felkészülés költségét és annak veszélyét, hogy későn reagál egy új követelményre.

A „legszigorúbb szabály mindenhova” megoldás könnyebben egységesítheti a megfelelést, de költséges és a helyi üzleti folyamatokra nézve túl korlátozó lehet. A jelentés szerint a szabályok géppel olvashatóvá tétele és az adatok eredetének, jellegének, céljának megőrzése segítheti az automatizált megfelelést. Az MI-rendszert érintő folyamatban minden modellnek és alrendszernek ismernie kell a feldolgozott adat kontextusát.

Digitális szuverenitás

Az adatok, a felhő, a számítási kapacitás és az MI-ökoszisztémák feletti ellenőrzés egyre inkább geopolitikai kérdés. A szervezeteknek egyensúlyt kell teremteniük a költséghatékonyság, az ellátásbiztonság, a helyi jogi követelmények és a technológiai önállóság között. A digitális szuverenitásra irányuló törekvések befolyásolhatják, hol tárolható és dolgozható fel adat, milyen szolgáltató vehető igénybe, illetve mennyire függ a szervezet egyetlen országtól vagy platformtól.

Harmadik félre támaszkodás

A felhő-, titkosítási, azonosítási, levelezési és más kritikus szolgáltatások külső szolgáltatókhoz kötődnek. A digitális kockázati index válaszadóinak 18%-a a beszállítói összekapcsoltságot a három legfontosabb kockázata közé sorolta. A szabályozási töredezettség a beszállítók kiválasztását és auditját is nehezíti: a szélesebb felmérésben 47% jelezte ezt problémaként.

A szervezet a kockázatért való felelősséget nem tudja a szolgáltatóra áthárítani. Folyamatos felügyeletre, átvilágításra, szerződéses hozzáférési és incidensjelentési jogokra, kilépési tervre és helyettesítő megoldásokra van szükség. A koncentrációs kockázatot is mérni kell, mivel egyetlen szolgáltató kiesése több üzleti funkciót egyidejűleg érinthet.

Irányítás, szakértelem és befektetési kényszer

Az irányítási modellek érettsége

A gyorsan változó digitális környezet a széttagolt irányítási modellektől az összehangoltabb működés felé tereli a szervezeteket. A jelentés három érettségi szintet különít el. Az analóg modell hagyományos, elkülönült funkciókra épül. A bővülő modell megtartja a szakterületi felelősséget, de több együttműködést és közös folyamatot hoz létre. Az összehangolt modell a digitális irányítást szervezeti szinten integrálja.

35%	48%	17%
analóg megközelítés	bővülő, együttműködésre épülő megközelítés	összehangolt irányítás

Az analóg működés önmagában nem jelenti azt, hogy nincs befektetés vagy szakértelem. Egyes ágazatokban és joghatóságokban a hagyományos funkciók megfelelhetnek a jelenlegi igényeknek. Ugyanakkor a koordináció hiánya elmoshatja a felelősséget, lassíthatja a döntéseket, és ideiglenes, incidensre reagáló megoldásokat eredményezhet. Az összehangolás célja, hogy az adatvédelmi, biztonsági, MI- és üzleti szempontok közös kockázati képpé álljanak össze.

Szakember- és költségvetési igény

A szakemberhiányt és az erőforrások elégtelenségét a válaszadók 20%-a emelte ki a Digitális Kockázati Indexben. A szélesebb felmérés válaszadóinak 23%-a a képzett munkatársak hiányát tartotta a digitális irányítás megvalósítása akadályának, 15% pedig a növekvő szabályozási terhek mellett költségvetési korlátokról számolt be. Az MI- és kiberbiztonsági tapasztalat iránti verseny a felvételt és a megtartást is megnehezíti.

A pénzhiány akadályozhatja az adatleltár korszerűsítését, a beszállítói felügyeletet, a megfelelő kontrollok kiépítését és a tehetségek felvételét. Ez a megtakarítás rövid távon kedvezőnek tűnhet, de hosszabb távon növelheti az incidensek, a megfelelési hibák és az elavult folyamatok költségét.

Az innováció elmulasztásának kockázata

A szervezeteknek nemcsak a technológia bevezetéséből eredő veszélyeket kell mérlegelniük. A túlzott késlekedés termelékenységi, ügyfélélménybeli és piaci hátrányt okozhat. Az új technológiák gyors fejlődése miatt a kockázati étvágyat rendszeresen felül kell vizsgálni, nem elegendő azt ritka éves ciklusban meghatározni. A vezetőknek mérlegelniük kell, milyen kontroll mellett vállalható egy kísérlet, milyen eredmény esetén bővíthető, és milyen feltételeknél kell leállítani.

Az MI-befektetés indoka

A jelentés iparági példákkal mutatja be, hogy az MI gyorsíthatja a gyógyszerkutatást, javíthatja a betegellátást, hatékonyabbá teheti a klinikai vizsgálatokat, és növelheti a működési termelékenységet. Ugyanakkor a versenytársak gyorsabb vagy eredményesebb alkalmazása piaci lemaradást okozhat. A befektetés így egyszerre versenyképességi döntés és kockázatkezelési feladat. A szabályozás, az adatminőség és az emberi felügyelet korai beépítése támogatja a fenntartható bevezetést.

Szervezeti válaszok: struktúra és kockázatalapú működés

Szerkezeti változások

A megkérdezettek közel fele már létrehozott digitális irányítási vagy hasonló funkciót, további 11% pedig azt tervezi, hogy a következő évben megteszi. Az adatirányítási, adatvédelmi, MI-irányítási, kiberbiztonsági és információbiztonsági bizottságok egyre gyakrabban jelentenek a felső vezetésnek vagy az igazgatóságnak. Több szervezet a korábban egymástól különálló csapatokat közös irányítási rendbe szervezi.

A fejlesztési prioritások is szélesednek. A magánszférán és az MI-irányításon kívüli beruházások közül 41% az adatirányítást, 35% a szabályozási megfelelésként kezelt kiberbiztonságot emelte ki. A fogyasztóvédelem, az emberi jogi kérdések, a platformfelelősség és az online biztonság kisebb, de szintén megjelenő területek. Ez a kormányzási feladatok összeolvadását jelzi.

A kockázatalapú megközelítés és az azt támogató eszközök

A modern digitális szabályozás egyre inkább a kockázat súlyosságához, valószínűségéhez és kontextusához igazítja az elvárásokat. A szervezeteknek ezért előzetesen kell értékelniük, hogy egy rendszer milyen hatással lehet az érintettekre, az üzletmenetre és az alapvető jogokra. Ez a működés dokumentált felelősséget igényel a fejlesztés, beszerzés, bevezetés és felülvizsgálat teljes életciklusában.

A vezetők beszámolói szerint a kockázatkezelés kevésbé silózottá válik. A különálló kiberbiztonsági, adatvédelmi és pénzügyi kockázati adatbázisok helyett közös vagy kevés számú rendszert használnak. A meglévő adatvédelmi hatásvizsgálat például kiindulópontot adhat az MI-hatásvizsgálathoz. Az automatizált értékelő eszközök besorolást, kockázati pontszámot, szabályzati sablont és kockázatcsökkentési javaslatot készíthetnek.

25%	43%
átlagosan a feladatok ekkora részénél használnak legalább részleges automatizálást	egyes konkrét folyamatok automatizálása eddig az arányig jutott

Az eszközök a fejlesztői folyamatokba és az új termékek munkamenetébe építve folyamatos auditnyomot hozhatnak létre. Ezzel csökkenhet a kézi adminisztráció, és a kockázatértékelés közelebb kerülhet a termékdöntésekhez. Az automatizálás azonban csak jó minőségű adatokra, átlátható szabályokra és érdemi emberi felülvizsgálatra támaszkodva ad megbízható eredményt.

Szervezeti válaszok: adatok és emberek

Az adatirányítás bővítése

Az MI-modell kimenete nem lehet megbízhatóbb, mint az alapjául szolgáló adat. A szervezetek ezért az adatirányítást az MI skálázásának alapvető feltételévé teszik. Az adatforrás, a jogszerűség, a pontosság, a címkézés és a származás nyilvántartása segít feltárni a hibás vagy torz adatkészleteket, valamint csökkenti a hallucináció, az elfogultság és az adatvédelmi jogsértés veszélyét.

Az adatvédelmet növelő technológiák támogatják az adatok biztonságos feldolgozását, illetve kevésbé érzékeny vagy mesterséges adatok előállítását. A felmérésben a biztonságos végrehajtási környezet és a szintetikus adat egyaránt 35%-kal szerepelt. A differenciális adatvédelem használata 25%, a federált tanulásé 15%, a homomorf titkosításé 9% volt. A válaszadók az innovációt és a versenyelőnyt is említették e technológiák alkalmazásának indokaként.

A már meglévő adatvédelmi munka adósságai is előtérbe kerültek. Az adatok címkézése és eredetének igazolása nem új feladat, de az MI nagyobb léptékben és több rendszer között teszi sürgetővé a rendezését. A korábban felhalmozódott hiányosságok pótlása lassíthatja a bevezetést, de stabilabb alapot ad a modellek biztonságos használatához.

Tehetség megszerzése és képzése

A szervezetek olyan szakembereket keresnek, akik mély szakterületi tudás mellett együtt tudnak dolgozni jogi, technológiai, adatkezelési, biztonsági és üzleti csapatokkal. Közel egyharmaduk további digitális kormányzási szakemberek felvételét tervezi. Ugyanakkor a korlátozott szakemberkínálat és a költségvetési nyomás miatt a toborzás lassú és drága lehet.

Az egyik válasz a belső képzés és a hibrid felelősségi szerepek létrehozása. Digitális felelősök vagy úgynevezett bajnokok működhetnek az egyes üzleti területeken, összekötve a helyi csapatot a központi irányítási funkciókkal. Így hamarabb jelezhetők a lehetőségek és a kockázatok, a képzés pedig fejleszti a munkatársakat és segítheti a megtartásukat.

A szélesebb felmérésben a szervezetek kétharmada számolt be digitális irányítási programja növekedéséről az elmúlt évben, miközben aktív toborzást közel egyharmaduk végzett. A növekvő feladat tehát gyakran gyorsabban bővül, mint a dedikált létszám. A meglévő munkatársak felkészítése és a felelősségek pontos elosztása ezért a kapacitásépítés fontos része.

Előretekintés

A digitális kockázatkezelés következő szakasza

A digitális kockázati környezetet a technológiai lehetőségek gyors növekedése, a szervezeti erőforrások korlátozottsága és a szabályozás széttagoltsága közötti feszültség határozza meg. A jelentés szerint a digitális kockázatot már nem lehet a megfelelésre összpontosító, önálló funkcióként kezelni. A vállalatok átalakítják kockázatkezelési folyamataikat és irányítási szerkezeteiket, miközben a digitális kockázat egyre magasabb vezetői és igazgatósági szintre kerül.

A kizárólag statikus kockázatcsökkentésre építő szervezet könnyen megbénulhat a szabályozási összetettségtől, a MI-vel támogatott kifinomult kibertámadásoktól, vagy lemaradhat azoktól a versenytársaktól, amelyek a kockázatvállalást és az innovációt kiegyensúlyozzák. A vezetőknek nemcsak azt kell megkérdezniük, hogyan előzzék meg a károkat, hanem azt is, miként lehet biztonságosan megvalósítani a hasznos technológiai kezdeményezéseket.

A fenntartható digitális innováció alapjai

A jövőbeli digitális felelősséghez robusztus irányítási struktúrák és több szakterületet összekötő szakértelem szükséges. Az adatirányítás, a kiberbiztonság, a beszállítói felügyelet, az adatvédelem és az MI-kontrollok közös működési rendbe illesztése növeli a döntések átláthatóságát. A fejlesztésbe épített értékelés és a folyamatos felügyelet lehetővé teszi, hogy az új felhasználási esetek örököljék az alapvető biztonsági és elszámoltathatósági kontrollokat.

A digitális kockázati funkció így a fenntartható versenyképesség és innováció előmozdítójává válhat. Ennek feltétele, hogy a felelősségi körök világosak legyenek, az adat és a technológia eredete nyomon követhető maradjon, és a szervezet rendszeresen újraértékelje kockázati étvágyát. Az egyszeri szabályzat vagy bizottsági jóváhagyás nem helyettesíti a napi működésbe épített felelősséget.

KÖRNYEZET	SZERVEZETI KÉPESSÉG	VÁRHATÓ EREDMÉNY
MI és automatizálás szabályozási eltérések geopolitikai kitettség	összehangolt irányítás megbízható adat képzett, együttműködő csapat	ellenőrizhető döntés reziliensebb működés vállalható innováció

A százalékos adatok a jelentés különböző felméréseiből és válaszadói köreiből származnak. Eltérő kérdésfeltevés és minta miatt az értékek közvetlen összehasonlítása csak a megadott kontextus figyelembevételével helyes.