



OSNOVNA ŠOLA  
POHORSKEGA ODREDA  
SLOVENSKA BISTRICA



# Umetna inteligenca in kibernetika varnost

## Računalništvo Raziskovalna naloga

**Avtor naloge:**

Naj Strmšek

**Mentor naloge:**

Vili Krajnc

Slovenska Bistrica, 2025

## ZAHVALA

Za izdelano raziskovalno nalogo gre zahvala predvsem mentorju Viliju Krajncu, profesorju tehnike in tehnologije ter fizike in ROIDu, ki me je skozi raziskovanje usmerjal in vzpodbujal.

Hkrati se zahvaljujem tudi vsem podjetjem in ustanovam, ki so sodelovala v anketi, kljub njeni občutljivi tematiki, kot je kibernetika varnost, saj brez njihove pomoči ta raziskovalna naloga ne bi mogla biti izvedena.

Hvala tudi staršem, ki so me skozi raziskovanje podpirali, spodbujali in mi omogočali nemoteno delo.

## KAZALO VSEBINE

1 UVOD .....	6
1.1 HIPOTEZE .....	8
2 TEORETIČNI DEL .....	10
2.1 UMETNA INTELIGENCA .....	10
2.1.1 Uvod v umetno inteligenco .....	10
2.1.2 Zgodovina umetne inteligence .....	10
2.1.3 Sodobni trendi in razvoj umetne inteligence.....	11
2.1.4 Vpliv umetne inteligence na gospodarstvo.....	12
2.1.5 Pomen kakovostnih podatkov in etična vprašanja .....	13
2.1.6 Uporaba umetne inteligence v različnih panogah .....	14
2.1.7 Umetna inteligenca v Sloveniji .....	14
2.1.8 Izzivi in prihodnost umetne inteligence.....	15
2.2 UMETNA INTELIGENCA V KIBERNETSKE VARNOSTI.....	16
2.2.1 Razširjenost umetne inteligence v kibernetški varnosti po svetu .....	16
2.2.2 Prednosti uporabe umetne inteligence v kibernetški varnosti .....	18
2.2.3 Microsoftovo letno poročilo o kibernetški varnosti.....	19
Poročilo 2023.....	20
Poročilo 2024.....	25
3 RAZISKOVALNI DEL .....	29
3.1 METODE RAZISKOVANJA.....	29
3.1.1 Preučevanje literature.....	29
3.1.2 Spletna anketa.....	29
3.2 ANALIZA ANKETNEGA VPRAŠALNIKA .....	29
3.2.1 Analiza ankete .....	29
3.2.2. Vprašanja.....	30
4 RAZPRAVA .....	51
5 ZAKLJUČEK.....	55
6 VIRI IN LITERATURA.....	57
7 PRILOGE.....	58
Priloga 1.....	58

## KAZALO SLIK

SLIKA 1: VIZUALNI PRIKAZ UMETNE INTELIGENCE.....	10
SLIKA 2: PRIKAZ TURINGOVEGA TESTA.....	11
SLIKA 3: VELIKOST TRGA UMETNE INTELIGENCE OD 2023 DO 2034.....	12
SLIKA 4: PREDVIDENI PRISPEVEK UMETNE INTELIGENCE K BDP PO REGIJAH NA SVETOVNI RAVNI .....	13
SLIKA 5: ZAKON O UMETNI INTELIGENCI EU: RAVNI TVEGANJA .....	13
SLIKA 6: ZA UMETNO INTELIGENCO DO LETA 2025 110 MILIJONOV EVROV .....	15
SLIKA 7: DELEŽ ORGANIZACIJ, KI SE ZANAŠAJO NA UMETNO INTELIGENCO (UI) ZA KIBERNETSKO VARNOST V IZBRANIH DRŽAVAH PO PANOGAH, STANJE V LETU 2019.....	16
SLIKA 8: VISOKA STOPNJA UPORABE UI ZA PREDVIDEVANJE IN ODGOVORE V KIBERNETSKI VARNOSTI .....	17
SLIKA 9: NAJPOGOSTEJŠI PRIMERI UPORABE UMETNE INTELIGENCE ZA KIBERNETSKO VARNOST V ORGANIZACIJAH V IZBRANIH DRŽAVAH, STANJE V LETU 2019.....	18
SLIKA 10: KOT DEL NAŠE DOLGOROČNE ZAVEZANOSTI USTVARJANJU VARNEJŠEGA SVETA, MICROSOFTOVA VLAGANJA V RAZISKAVE NA PODROČJU VARNOSTI, INOVACIJE IN GLOBALNO VARNOSTNO SKUPNOST VKLJUČUJEJO.....	20
SLIKA 11: OSNOVE KIBERNETSKÉ HIGIENE.....	20
SLIKA 12: POGLED NA PODROČJE IZSILJEVALSKIH NAPADOV .....	21
SLIKA 13: KAKO SE PODROČJE GROŽENJ RAZVIJA .....	21
SLIKA 14: ŠTEVILO DNEVNIH POSKUSOV KOMPROMISOV POSLOVNE E-POŠTE OD APRILA 2022 DO APRILA 2023 .....	22
SLIKA 15: NAJBOLJ CILJNE DRŽAVE PO REGIJAH .....	22
SLIKA 16: DELEŽ RANLJIVIH IN NERANLJIVIH IOT NAPRAV.....	23
SLIKA 17: UI IN VELIKI JEZIKOVNI MODELI (LLM) BODO SPREMENILI KIBERNETSKO VARNOST .....	23
SLIKA 18: GRAFIKON - 50-ODSTOTNO ZMANJŠANJE VLOMLJENIH STREŽNIKOV COBALT STRIKE V ZDA .....	24
SLIKA 19: V ZADNJEM LETU SE JE POVPRASEVANJE PO STROKOVNJAKIH ZA KIBERNETSKO VARNOST POVEČALO ZA 35% .....	24
SLIKA 20: 3-KRATNO ZMANJŠANJE NAPADOV NA STOPNJI ODKUPNINE KLJUB 2,75-KRATNEMU POVEČANJU ŠTEVILA SREČANJ .....	25
SLIKA 21: DNEVNI OBSEG ZLONAMERNEGA PROMETA.....	25
SLIKA 22: VEČ KOT 99 % NAPADOV NA IDENTITETO SO NAPADI Z GESLI .....	26
SLIKA 23: KRIPTOVALUTE, KI SO JIH UKRADLI SEVERNO KOREJSKI HEKERJI .....	26
SLIKA 24: 10 NAJBOLJ NAPADENIH SEKTORJEV NA SVETU .....	27
SLIKA 25: SPOSOBNOST SOVRAŽNE UPORABE UMETNE INTELIGENCE Z NAMENOM SPLETNEGA VPLIVA .....	27
SLIKA 26: PANOGA PODJETIJ .....	30
SLIKA 27: ŠTEVILO ZAPOSLENIH.....	31
SLIKA 28: UPORABA UMETNE INTELIGENCE.....	32
SLIKA 29: PODROČJE UPORABE UMETNE INTELIGENCE.....	33
SLIKA 30: POGOSTOST UPORABE UMETNE INTELIGENCE .....	34
SLIKA 31: UPORABA UMETNE INTELIGENCE ZA ZAŠČITO PRED KIBERNETSKIMI GROŽNJAMI.....	35
SLIKA 32: PODROČJA KIBERNETSKÉ VARNOSTI KJER SE UPORABLJA UMETNA INTELIGENCA .....	36
SLIKA 33: PREDNOSTI UPORABE UMETNE INTELIGENCE NA PODROČJU KIBERNETSKÉ VARNOSTI .....	37
SLIKA 34: GLAVNE OVIRE ZA ŠIRŠO UPORABO UMETNE INTELIGENCE NA PODROČJU KIBERNETSKÉ VARNOSTI .....	38
SLIKA 35: VPLIV UPORABE UMETNE INTELIGENCE NA PODROČJU KIBERNETSKÉ VARNOSTI NA STROŠKE.....	39
SLIKA 36: POMEMBOST UPORABE UMETNE INTELIGENCE ZA IZBOLJŠANJE KIBERNETSKÉ VARNOSTI.....	40
SLIKA 37: OCENA UČINKOVITOSTI UI V KIBERNETSKI VARNOSTI V PRIMERJAVI S TRADICIONALNIMI METODAMI .....	41
SLIKA 38: POMEMBOST UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI V PRIHODNOSTI .....	43
SLIKA 39: PORAST NAPADOV NA STREŽNIKE, KI VKLJUČUJEJO UPORABO UMETNE INTELIGENCE .....	43
SLIKA 40: PRIPRAVE NA OBRAMBO PRED NAPADI, KI VKLJUČUJEJO UMETNO INTELIGENCO .....	44
SLIKA 41: OCENA PRIPRAVLJENOSTI PRED KIBERNETSKIMI NAPADI, KI VKLJUČUJEJO UPORABO UI .....	45
SLIKA 42: OCENA POMEMBOSTI STROŠKA IMPLEMENTACIJE NA UVEDBO UMETNE INTELIGENCE .....	47
SLIKA 43: OCENA POMEMBOSTI RAZPOLOŽLJIVOSTI STROKOVNJAKOV NA UVEDBO UMETNE INTELIGENCE ...	48
SLIKA 44: OCENA POMEMBOSTI ZAUPANJA V TEHNOLOGIJO NA UVEDBO UMETNE INTELIGENCE.....	49
SLIKA 45: OCENA POMEMBOSTI PODPORE VODSTVA NA UVEDBO UMETNE INTELIGENCE .....	50

## **POVZETEK**

V raziskovalni nalogi sem preučil vlogo umetne inteligence (UI) v kibernetški varnosti ter njen vpliv na informacijske sisteme v podjetjih v Sloveniji. Zanimalo me je, v kolikšni meri podjetja že uporabljajo UI za zaščito pred kibernetškimi napadi, kakšne so prednosti in izzivi njene implementacije ter kakšna je prihodnost te tehnologije na področju kibernetške varnosti.

V teoretičnem delu sem predstavil razvoj UI, njene sodobne trende in uporabo v različnih panogah. Podrobneje sem raziskal njeno vlogo v kibernetški varnosti, kjer omogoča hitrejše odkrivanje groženj, avtomatizacijo varnostnih procesov in analizo napadov v realnem času. Kljub številnim prednostim pa uporaba UI prinaša tudi izzive, kot so visoki stroški, pomanjkanje strokovnjakov in nezaupanje vanjo.

V raziskovalnem delu sem izvedel anketo med slovenskimi podjetji in ugotovil, da večina že uporablja ali načrtuje uporabo UI v kibernetški varnosti. Kot glavne prednosti so anketiranci navedli hitrejšo detekcijo groženj in avtomatizacijo procesov, medtem ko so največje ovire visoki stroški in pomanjkanje kadra.

Moje ugotovitve se skladajo z literaturo iz teoretičnega dela. Večina anketirancev verjame, da bo UI v prihodnosti ključna pri zaščiti pred kibernetškimi napadi, vendar bo za njeno širšo implementacijo potrebno še veliko prilagoditev in investicij.

Za ponazoritev uporabe umetne inteligence sem pri pripravi tega povzetka uporabil orodje ChatGPT, ki mi je pomagal tudi pri njegovem prevodu.

**Ključne besede:** umetna inteligenca, kibernetška varnost, kibernetški napadi

## **ABSTRACT**

In my research paper, I examined the role of artificial intelligence (AI) in cybersecurity and its impact on information systems in Slovenian companies. I was interested in the extent to which companies already use AI for protection against cyberattacks, the advantages and challenges of implementing it, and the future of this technology in cybersecurity.

In the theoretical part, I presented the development of AI, its modern trends, and its applications in various industries. I specifically explored its role in cybersecurity, where it enables faster threat detection, automation of security processes, and real-time attack analysis. Despite its numerous advantages, the use of AI also presents challenges, such as high costs, a shortage of experts, and distrust in its reliability.

In the research section, I conducted a survey among Slovenian companies and found that most already use or plan to use AI in cybersecurity. The main advantages cited by respondents were faster threat detection and process automation, while the biggest obstacles were high costs and a shortage of skilled personnel.

My findings align with the literature from the theoretical part. Most respondents believe that AI will be crucial for protecting against cyberattacks in the future. However, its broader implementation will require significant adjustments and investments.

To further illustrate the use of artificial intelligence, I used ChatGPT tool to help me prepare this summary, as well as to translate it.

**Keywords:** artificial intelligence, cybersecurity, cyberattacks

## 1 UVOD

Umetna inteligenca (UI) je področje računalništva, ki se osredotoča na razvoj sistemov, sposobnih za izvajanje nalog, ki običajno zahtevajo človeško inteligenco. Sem spadajo naloge, kot so prepoznavanje govora, obdelava naravnega jezika, vizualno prepoznavanje in odločanje. UI temelji na algoritmih, ki omogočajo računalnikom, da se učijo iz podatkov in se prilagajajo novim situacijam brez neposrednega programiranja. V zadnjih letih se je UI izredno hitro razvijala, kar je omogočilo njen preboj v različna področja, kot so medicina, finance, avtomobilska industrija, kibernetška varnost in druge.

Kibernetška varnost zajema zaščito računalniških sistemov, omrežij in podatkov pred napadi, škodo ali nepooblaščenim dostopom. S širjenjem uporabe digitalnih tehnologij v vseh vidikih družbe postajajo sistemi in podatki vedno bolj ranljivi za kibernetške napade, ki lahko ogrozijo zasebnost in varnost posameznikov, podjetij in držav. Kibernetška varnost se zato osredotoča na preprečevanje, odkrivanje in odzivanje na te grožnje z uporabo različnih orodij, tehnik in protokolov.

V zadnjih letih je uporaba umetne inteligence postala ključni dejavnik v izboljšanju kibernetške varnosti. UI omogoča hitro prepoznavanje vzorcev napadov, samodejno prepoznavanje ranljivosti v sistemih ter izvajanje naprednih metod za analizo groženj. Prav tako omogoča hitrejšo obdelavo podatkov, kar pripomore k večji učinkovitosti v boju proti kibernetškim napadom. Hkrati pa se pojavljajo tudi novi izzivi, saj napadalci uporabljajo UI za razvoj bolj sofisticiranih napadov, kar pomeni, da mora biti kibernetška varnost natančno usmerjena in stalno posodobljena, da bi ostala korak pred temi grožnjami.

Ta raziskovalna naloga obsega raziskavo o uporabi umetne inteligence na področju kibernetške varnosti v Sloveniji, izzivih njene implementacije, potencialne možnosti v prihodnosti in njeno uporabo za kibernetške napade. S pomočjo ankete bom poizkušal pridobiti informacije o trenutnem stanju umetne inteligence na področju kibernetške varnosti ter podatke zbral in jih predstavil v nadaljevanju. To temo sem si izbral zato, ker je aktualna in primerna času, v katerem živimo, ki je vedno bolj usmerjen k uporabi umetne inteligence v vseh vidikih človekovega življenja in razvoja, hkrati pa se vsej tehnologiji navkljub, ali pa prav zaradi nje, dogaja na milijone kibernetških napadov

letno. Dodaten razlog za izbor teme raziskovalne naloge je tudi dejstvo, da to področje v Sloveniji še ni zelo raziskano.

Zelo sem vesel, da sem si izbrali to temo, saj sem odkrili zanimive rezultate, ki so nekatere moje hipoteze potrdili, druge pa ovrgli.

## 1.1 HIPOTEZE

V raziskavi sem najprej določil širše zastavljena raziskovalna vprašanja:

1. Ali podjetja v Sloveniji že uporabljajo umetno inteligenco za napovedovanje, prepoznavanje in odzivanje na kibernetške napade?
2. Kako pogosto podjetja v Sloveniji uporabljajo storitve umetne inteligence (UI) za izboljšanje kibernetške varnosti?
3. Kakšen potencial vidijo podjetja v Sloveniji v uporabi umetne inteligence za zaščito pred kibernetškimi grožnjami?
4. Kakšne so prednosti in slabosti uporabe umetne inteligence v kibernetški varnosti, po mnenju strokovnjakov?
5. Kakšne so ovire za širšo uporabo umetne inteligence v podjetjih v Sloveniji?
6. Ali podjetja menijo, da je uporaba umetne inteligence mogoča za kibernetške napade v prihodnosti?
7. Kako se podjetja v Sloveniji pripravijo na obrambo pred napadi, ki vključujejo umetno inteligenco?
8. Kakšen vpliv ima uporaba umetne inteligence v kibernetški varnosti na stroške in kompleksnost obrambnih sistemov?
9. Ali podjetja v Sloveniji opažajo naraščajoče se število napadov, ki vključujejo umetno inteligenco?

Zgornja raziskovalna vprašanja so mi služila kot podlaga, na osnovi katere sem postavil sledeče hipoteze:

**H1:** Večina podjetij v Sloveniji že uporablja umetno inteligenco.

**H2:** Podjetja za kibernetško varnost v Sloveniji že uporabljajo umetno inteligenco, vendar v omejenem obsegu.

**H3:** Večina slovenskih podjetij meni, da umetna inteligenca predstavlja velik potencial za izboljšanje kibernetške varnosti.

**H4:** Glavna ovira za širšo uporabo umetne inteligence v kibernetški varnosti pri slovenskih podjetjih so visoki stroški implementacije in pomanjkanje strokovnjakov.

**H5:** Podjetja, ki uporabljajo umetno inteligenco, dosegajo hitrejše in natančnejše odkrivanje kibernetških groženj.

**H6:** Podjetja v Sloveniji se soočajo z večjimi izzivi pri obrambi pred napadi, ki uporabljajo umetno inteligenco zaradi njene naprednosti.

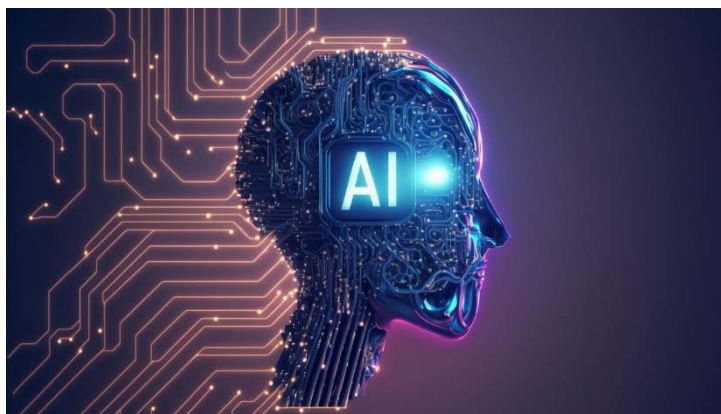
**H7:** Podjetja v Sloveniji vlagajo v UI rešitve in izvajajo redna usposabljanja zaposlenih.

## 2 TEORETIČNI DEL

### 2.1 UMETNA INTELIGENCA

#### 2.1.1 Uvod v umetno inteligenco

Umetna inteligenca (UI) je tehnologija, ki omogoča računalnikom in sistemom, da opravljajo naloge, ki običajno zahtevajo človeško inteligenco, kot so prepoznavanje govora, učenje, odločanje in reševanje problemov. Z nenehnim razvojem in izboljšavami v računalniški tehnologiji je UI postala pomemben del različnih industrij in panog, vključno z zdravstvom, financami, trgovino, izobraževanjem ipd. S svojo sposobnostjo analize velikih količin podatkov lahko UI pomaga izboljšati poslovne procese, optimizirati odločanje ter povečati produktivnost in učinkovitost.



Slika 1: Vizualni prikaz umetne inteligence<sup>1</sup>

#### 2.1.2 Zgodovina umetne inteligence

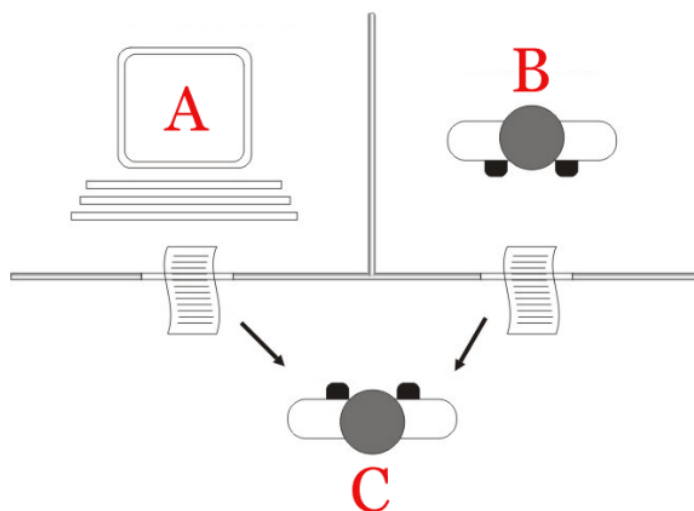
Razvoj umetne inteligence sega v sredino 20. stoletja, ko so znanstveniki začeli razvijati prve teoretične koncepte in računalniške algoritme, ki bi omogočili simulacijo človeškega mišljenja. Eden prvih primerov UI je bil Alan Turingov test (slika 2), znan kot Turingov test, ki je preizkusil sposobnost računalnika, da posnema človeško inteligenco.

Pri testu človeški ocenjevalec presoja besedilni prepis pogovora v naravnem jeziku med človekom in strojem. Ocenjevalec poskuša prepoznati stroj, pri čemer ga ta uspešno prestane, če ocenjevalec ne more zanesljivo razlikovati med njima.

---

<sup>1</sup> <https://www.zabala.eu/wp-content/uploads/2023/11/Artificial-inteligente-and-consultancy-1200x675.jpg>

Skozi desetletja so se pojavili različni pristopi in metode, kot so strojno učenje, globoko učenje in naravni jezikovni procesi, ki so omogočili hitrejši napredek in širšo uporabo UI na različnih področjih.



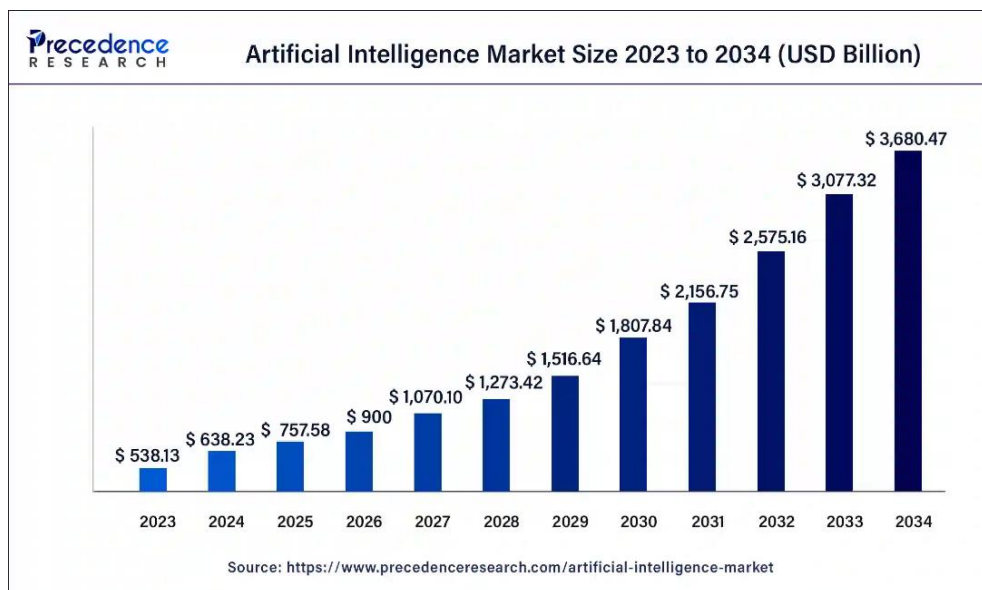
Slika 2: Prikaz Turingovega testa<sup>2</sup>

### 2.1.3 Sodobni trendi in razvoj umetne inteligence

V zadnjih desetletjih smo priča hitremu napredku na področju umetne inteligence, še posebej v povezavi z uporabo velikih količin podatkov, računalniške moči in naprednih algoritmov. Danes se umetna inteligenca uporablja za različne naloge, kot so prepoznavanje obrazov in govora, avtomatizacija delovnih procesov, napovedovanje trendov ter optimizacija produktivnosti. Uporaba UI je vse bolj prisotna v vsakdanjem življenju, od pametnih telefonov, kot so glasovni asistenti (npr. Siri, Google Assistant), do avtomobilov z avtonomno vožnjo in personaliziranih priporočil na spletnih platformah, kot so Netflix in Spotify.

---

<sup>2</sup> [https://en.wikipedia.org/wiki/Turing\\_test#/media/File:Turing\\_test\\_diagram.png](https://en.wikipedia.org/wiki/Turing_test#/media/File:Turing_test_diagram.png)



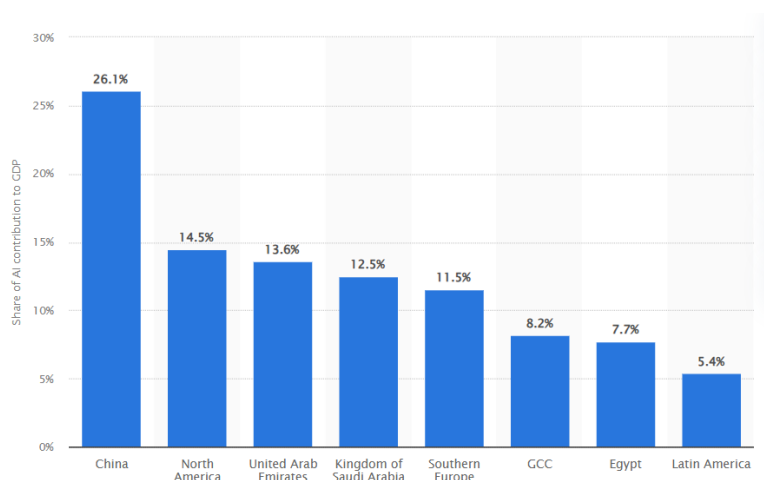
Slika 3: Velikost trga umetne inteligence od 2023 do 2034<sup>3</sup>

Graf (slika 3) prikazuje impresivno napovedano rast trga umetne inteligence med letoma 2023 in 2034. V letu 2023 je trg znašal približno 538,13 milijarde USD, medtem ko naj bi do leta 2034 dosegel kar 3680,47 milijarde USD. Ta rast odraža vse večje povpraševanje po UI rešitvah v različnih sektorjih, kot so zdravstvo, finance, logistika in izobraževanje. Zlasti hitro razvijajoča se tehnologija, kot je generativna umetna inteligenca, še dodatno pospešuje širitev trga in priložnosti za inovacije.

#### 2.1.4 Vpliv umetne inteligence na gospodarstvo

Umetna inteligenca ima lahko velik vpliv na gospodarstvo, saj omogoča podjetjem optimizacijo procesov, večjo produktivnost in ustvarjanje novih poslovnih modelov. Po ocenah analitikov naj bi umetna inteligenca do leta 2030 prispevala 11,5 % k bruto domačemu proizvodu (BDP) južne Evrope, kar pomeni, da bo njen vpliv na gospodarsko rast zelo pomemben. UI omogoča tudi povečanje ustvarjalnosti v podjetjih, saj omogoča hitro analizo podatkov in optimizacijo odločitev, kar pripomore k večji inovativnosti in hitrejšemu prilagajanju potrebam trga.

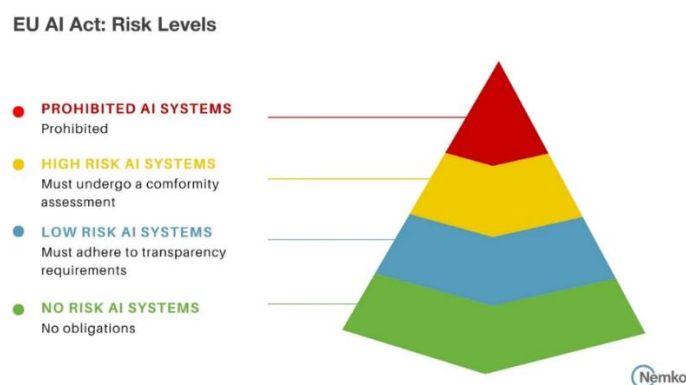
<sup>3</sup> <https://www.precedenceresearch.com/insightimg/artificial-intelligence-market-size.webp>



Slika 4: Predvideni prispevek umetne inteligence k BDP po regijah na svetovni ravni <sup>4</sup>

### 2.1.5 Pomen kakovostnih podatkov in etična vprašanja

Za uspešno delovanje umetne inteligence so ključni kakovostni podatki. Slabi ali nepopolni podatki lahko vodijo do napačnih odločitev, ki lahko negativno vplivajo na poslovanje. Zaradi tega je pomembno, da organizacije skrbijo za zbiranje in obdelavo podatkov na način, ki zagotavlja njihovo točnost in zanesljivost. Poleg tega se postavlja vprašanje etike pri uporabi umetne inteligence. Ker UI lahko sprejema odločitve, ki vplivajo na posameznike in družbo, je pomembno, da se razvijejo smernice za odgovorno uporabo in nadzor nad umetno inteligenco. Evropska unija je že sprejela zakonodajo, ki ureja odgovorno uporabo UI in zagotavlja varnost ter zaščito uporabnikov. (Fernández Peñalver, 2024)



Slika 5: Zakon o umetni inteligenci EU: Ravni tveganja<sup>5</sup>

<sup>4</sup> <https://cdn.statcdn.com/Statistic/1040000/1042325-blank-754.png>

<sup>5</sup> <https://www.nemko.com/hubfs/Overview%20of%20AI%20risk%20levels%20as%20defined%20by%20the%20EU%20AI%20Act.jpg>

### **2.1.6 Uporaba umetne inteligence v različnih panogah**

Umetna inteligenca se uporablja v številnih panogah. V zdravstvu omogoča hitrejšo diagnostiko bolezni, izboljšanje zdravljenja in boljše obvladovanje zdravstvenih storitev. V finančah UI pomaga pri analizi tveganj, napovedovanju finančnih trendov in avtomatizaciji procesov, kot je obvladovanje strankinih podatkov. V kmetijstvu se umetna inteligenca uporablja za optimizacijo pridelave in zmanjšanje porabe virov, medtem ko v avtomobilski industriji omogoča razvoj avtonomnih vozil. Vse to prispeva k večji učinkovitosti, zmanjšanju stroškov in izboljšanju kakovosti storitev.

### **2.1.7 Umetna inteligenca v Sloveniji**

V Sloveniji pa umetna inteligenca še vedno ni tako prisotna, kot v drugih razvitih državah. Raziskave, kot je tista Univerze v Ljubljani<sup>6</sup>, kaže, da le 25 % Slovencev redno uporablja napredne tehnologije, kot je generativna umetna inteligenca (ChatGPT, MidJourney, Gemini). (Praček & Vehovar, 2024)

Kljub temu so nekatera podjetja že začela uvajati UI, kot na primer podjetje Inovia, ki je razvilo rešitev za avtomatizacijo procesov, kar je pripomoglo k večji učinkovitosti in zmanjšanju napak v poslovanju. Microsoft v Sloveniji že aktivno sodeluje z različnimi podjetji, da spodbuja uporabo umetne inteligence z izobraževalnimi programi in pomočjo pri uvajanju teh tehnologij.

Tudi Slovenija je v zadnjih letih vedno bolj investirala v umetno inteligenco, kar kaže prikaz sredstev, ki jih je država namenila za umetno inteligenco med letoma 2021 in 2025 (Biljak Gerjevič, 2021).

---

<sup>6</sup> [https://www.uni-lj.si/assets/Kabinet/A-Novice/2024-12-19-raziskava-UI/Besedilo-raziskave-Umetna-inteligenca-v-Sloveniji-uporaba-in-staliska.pdf?utm\\_](https://www.uni-lj.si/assets/Kabinet/A-Novice/2024-12-19-raziskava-UI/Besedilo-raziskave-Umetna-inteligenca-v-Sloveniji-uporaba-in-staliska.pdf?utm_)

<b>ZA UMETNO INTELIGENCO DO LETA 2025 110 MILIJONOV EVROV</b>		
<b>Strateški cilj</b>	<b>Postavka (v EUR)</b>	<b>*Vir podatkov: NpUI</b>
Vpeljava umetne inteligence v gospodarstvo, javni sektor, javno in državno upravo ter družbo.	47.950.000	
Podpora raziskavam in inovacijam.	40.100.000	
Vzpostavitev tehnične infrastrukture.	11.580.000	
Izobraževanje in krepitev človeških virov.	4.100.000	
Okrepitev mednarodnega sodelovanja.	1.800.000	
Okrepitev varnosti z uporabo umetne inteligence.	1.500.000	
Povečanje zaupanja javnosti v umetno inteligenco.	1.500.000	
Zagotovitev ustreznega pravnega in etičnega okvira.	700.000	
Vzpostavitev ekosistema deležnikov.	400.000	
Vzpostavitev nacionalnega observatorija za umetno inteligenco v Sloveniji.	370.000	


Slika 6: Za umetno inteligenco do leta 2025 110 milijonov evrov<sup>7</sup>

### 2.1.8 Izzivi in prihodnost umetne inteligence

Kljub obetavnim primerom uporabe UI v Sloveniji slovenska podjetja še vedno zaostajajo za evropskim povprečjem pri uvajanju teh tehnologij, kot je pokazala raziskava podjetja Ranktracker<sup>8</sup>. En izmed večjih izzivov pri širši uporabi UI je premagovanje pomanjkanja znanja in izkušenj pri slovenskih podjetjih, ki bi omogočila prehod na digitalizirane poslovne modele. Kljub tem izzivom pa se zdi, da Slovenija s pomočjo podpornih programov in strateškega razvoja v prihodnosti še vedno lahko izkoristi potencial umetne inteligence za povečanje konkurenčnosti na globalnem trgu.

V prihodnosti se pričakuje, da bo umetna inteligenca postala pomemben dejavnik tako v gospodarskem razvoju Slovenije kot v različnih industrijskih sektorjih. Da bi Slovenija izkoristila vse prednosti, mora spodbujati večjo digitalno preobrazbo ter povečati uporabo UI v vseh panogah, kar bo omogočilo rast, inovacije in konkurenčnost na svetovnem trgu.

<sup>7</sup><https://n1info.si/wp-content/uploads/2021/06/30/1625045528-umetna-inteligenca-web-1024x576.png>

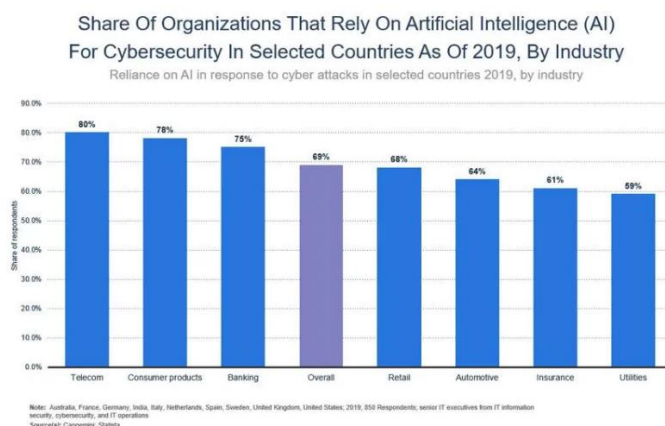
<sup>8</sup> <https://www.ranktracker.com/sl/blog/artificial-intelligences-role-in-cyber-security-revolution/>

## 2.2 UMETNA INTELIGENCA V KIBERNETSKI VARNOSTI

### 2.2.1 Razširjenost umetne inteligence v kibernetški varnosti po svetu

Uporaba umetne inteligence v kibernetški varnosti hitro narašča in postaja ključni element v boju proti kibernetškim grožnjam. Raziskave so pokazale, da podjetja na različnih področjih zaupajo umetni inteligenci pri odkrivanju, napovedovanju in odzivanju na napade.

Po raziskavi podjetja Capgemini<sup>9</sup> o uporabi umetne inteligence v kibernetški varnosti iz leta 2019 je 80 % vodilnih v telekomunikacijskih podjetjih prepričanih, da njihova organizacija ne bi bila sposobna učinkovito odgovarjati na kibernetške napade brez uporabe umetne inteligence. Še bolj presenetljiv je podatek, da 69 % višjih izvršnih direktorjev iz sedmih različnih industrij meni, da bi brez umetne inteligence njihove organizacije verjetno obtičale pri odzivu na napade. V bančnem sektorju je ta številka še višja: kar 75 % bančnih direktorjev meni, da bodo za preprečevanje kibernetških napadov potrebovali umetno inteligenco. Na drugi strani pa 59 % direktorjev v energetskih podjetjih, kar je najnižja številka v raziskavi, vidi umetno inteligenco kot ključno za obvladovanje kibernetških groženj. Energetska podjetja so med bolj ranljivimi sektorji zaradi svoje zastarele infrastrukture, kar jih postavlja v še večje tveganje za napade.



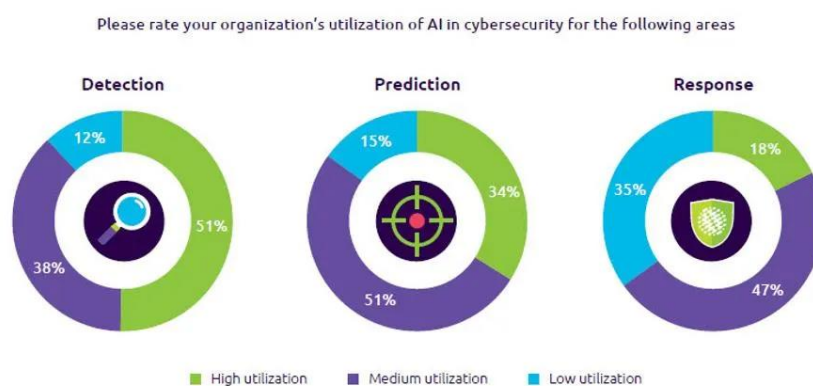
Slika 7: Delež organizacij, ki se zanašajo na umetno inteligenco (UI) za kibernetško varnost v izbranih državah po panogah, stanje v letu 2019<sup>10</sup>

<sup>9</sup> [https://www.capgemini.com/gb-en/wp-content/uploads/sites/5/2022/05/AI-in-Cybersecurity\\_Report\\_20190710\\_V05.pdf](https://www.capgemini.com/gb-en/wp-content/uploads/sites/5/2022/05/AI-in-Cybersecurity_Report_20190710_V05.pdf)

<sup>10</sup> <https://imageio.forbes.com/specials-images/imageserve/5dbfb8b8b4d505000678d1b3/10-Charts-That-Will-Change-Your-Perspective-Of-AI-In-Security/960x0.jpg?format=jpg&width=1440>

Umetna inteligenca se v podjetjih uporablja predvsem za odkrivanje groženj. Po podatkih raziskave iz leta 2019<sup>11</sup>, 51 % podjetij večinoma uporablja umetno inteligenco za prepoznavanje groženj, napovedovanje in odzivanje na njih. Medtem ko številna podjetja še vedno ostajajo pri osnovnem odkrivanju groženj, nekatera že napredujejo v fazo napovedovanja in odzivanja na grožnje, kar je področje, kjer se pojavljajo najbolj zanimivi projekti umetne inteligence, saj te naloge hitro širijo meje obstoječih tehnologij.

Figure 3: Higher utilization of AI for detection than prediction or response



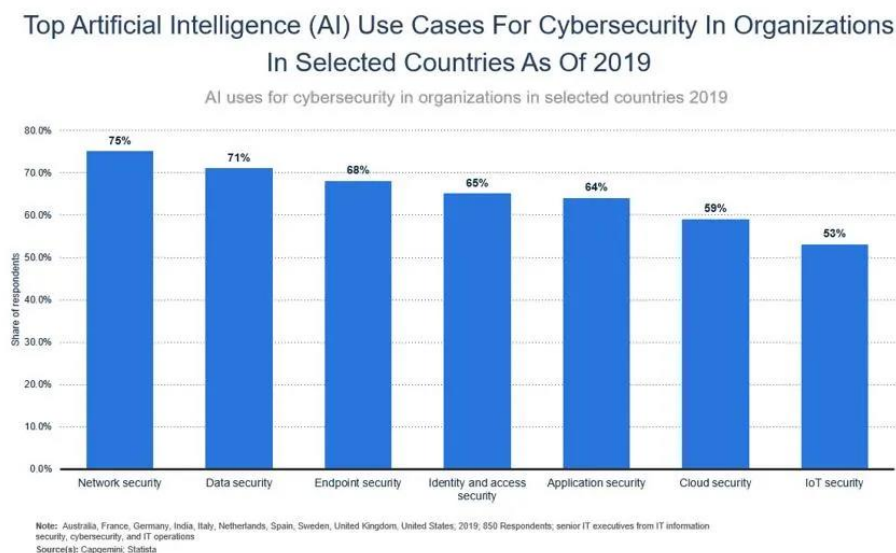
Source: Capterra Research Institute, AI in Cybersecurity executive survey, N = 850 executives

Slika 8: Visoka stopnja uporabe UI za predvidevanje in odgovore v kibernetški varnosti<sup>12</sup>

Poleg tega raziskava razkriva, da 75 % podjetij danes uporablja umetno inteligenco za omrežno varnost, kar je najpogostejša uporaba te tehnologije v kibernetški varnosti. Podjetja prav tako vse pogosteje uporabljajo UI za varnost podatkov (71 %) in varnost končnih točk (68 %). Grafikon spodaj (slika 9) prikazuje, kako je umetna inteligenca postala ključen del sedmih najpomembnejših strategij, ki jih podjetja uporabljajo v boju proti kibernetškim napadom.

<sup>11</sup> Raziskava omenjena v <https://www.forbes.com/sites/louiscolombus/2019/11/04/10-charts-that-will-change-your-perspective-of-ai-in-security/>

<sup>12</sup> <https://imageio.forbes.com/specials-images/imageserve/5dbfbef9b4d505000678d1b6/10-Charts-That-Will-Change-Your-Perspective-Of-AI-In-Security/960x0.jpg?height=423&width=711&fit=bounds>



Slika 9: Najpogostejši primeri uporabe umetne inteligence za kibernetško varnost v organizacijah v izbranih državah, stanje v letu 2019<sup>13</sup>

Umetna inteligenca tako postaja temelj za številne strategije kibernetške varnosti, saj omogoča podjetjem, da se hitreje prilagodijo novim grožnjam in učinkoviteje zaščitijo svoje sisteme pred napadi.

## 2.2.2 Prednosti uporabe umetne inteligence v kibernetški varnosti

Umetna inteligenca (UI) prinaša številne prednosti na področju kibernetške varnosti, ki organizacijam pomagajo pri učinkovitejšem odkrivanju in odzivanju na grožnje. Med ključnimi prednostmi so:

- 1. Izboljšano zaznavanje groženj:** Sistemi, ki temeljijo na UI, lahko analizirajo velike količine podatkov in prepoznajo anomalije ter potencialne grožnje v realnem času. Tradicionalne metode se pogosto soočajo z izzivi pri obdelavi ogromnih količin podatkov, ki jih ustvarjajo sodobna omrežja. Algoritmi UI lahko te podatke obdelajo hitreje, kar izboljša odkrivanje znanih in neznanih groženj.
- 2. Avtomatizacija varnostnih operacij:** UI omogoča avtomatizacijo rutinskih varnostnih nalog, kar zmanjšuje obremenitev varnostnih ekip in omogoča osredotočanje na bolj kompleksne grožnje. Po nekaterih ocenah je mogoče

<sup>13</sup> <https://imageio.forbes.com/specials-images/imageserve/5dbfc09aca425400079c5e22/10-Charts-That-Will-Change-Your-Perspective-Of-AI-In-Security/960x0.jpg?height=398&width=711&fit=bounds>

avtomatizirati skoraj 40 % vsakodnevnih varnostnih operacij, kar poudarja potencial UI pri izboljšanju delovnih procesov v kibernetški varnosti.

3. **Napovedovanje in proaktivno odzivanje na grožnje:** UI lahko na podlagi preteklih podatkov in vedenjskih vzorcev napadalcev napoveduje potencialne kibernetške napade. To omogoča organizacijam, da proaktivno ukrepajo in preprečijo napade, preden se ti zgodijo.
4. **Prilagodljivost in učenje:** Sistemi UI se lahko učijo iz novih podatkov in prilagajajo novim grožnjam, kar izboljšuje njihovo učinkovitost skozi čas. To pomeni, da lahko UI prepozna tudi nove vrste napadov, ki jih prej ni bilo mogoče zaznati.
5. **Zmanjšanje človeških napak:** Avtomatizacija z UI zmanjšuje možnost človeških napak pri odkrivanju in odzivanju na grožnje, saj sistemi delujejo dosledno in brez utrujenosti.

Kljub tem prednostim je pomembno poudariti, da UI ne more popolnoma nadomestiti človeškega dejavnika v kibernetški varnosti. Človeški strokovnjaki so še vedno ključni pri interpretaciji rezultatov, sprejemanju strateških odločitev in obravnavi kompleksnih varnostnih incidentov. Kombinacija UI in človeške ekspertize tako predstavlja najboljši pristop k učinkoviti kibernetški varnosti.

### **2.2.3 Microsoftovo letno poročilo o kibernetški varnosti**

V zadnjih letih je videti, da je vedno več govora o uporabi umetne inteligence za zagotavljanje kibernetške varnosti. Microsoft vsako objavi letno poročilo o kibernetški varnosti, ugotovitve iz zadnjih dveh (2023 in 2024) pa so nadaljevanju tudi povzete:

## Poročilo 2023



Slika 10: Kot del naše dolgoročne zavezanosti ustvarjanju varnejšega sveta, Microsoftova vlaganja v raziskave na področju varnosti, inovacije in globalno varnostno skupnost vključujejo<sup>14</sup>

**Osnovna varnostna higiena ostaja ključna:** Ugotovili so, da 99 % napadov lahko preprečimo z osnovnimi varnostnimi ukrepi, kot so omogočanje več faktorske avtentikacije (MFA), uporaba načela Zero Trust in redno posodabljanje programske opreme.



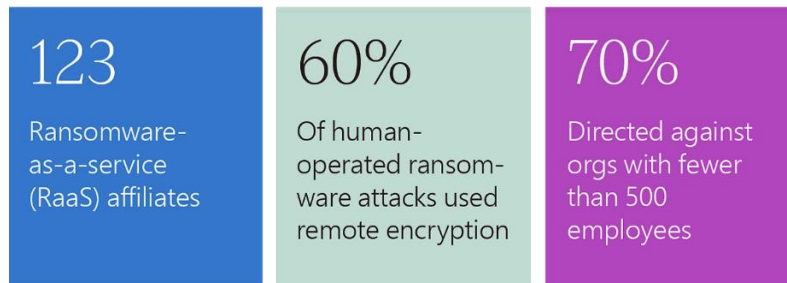
Slika 11: Osnove kibernetške higiene<sup>15</sup>

<sup>14</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_00\\_Microsofts-unique-vantage@2x-1-1?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_00_Microsofts-unique-vantage@2x-1-1?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

<sup>15</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_10\\_Basic-security-hygiene@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_10_Basic-security-hygiene@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

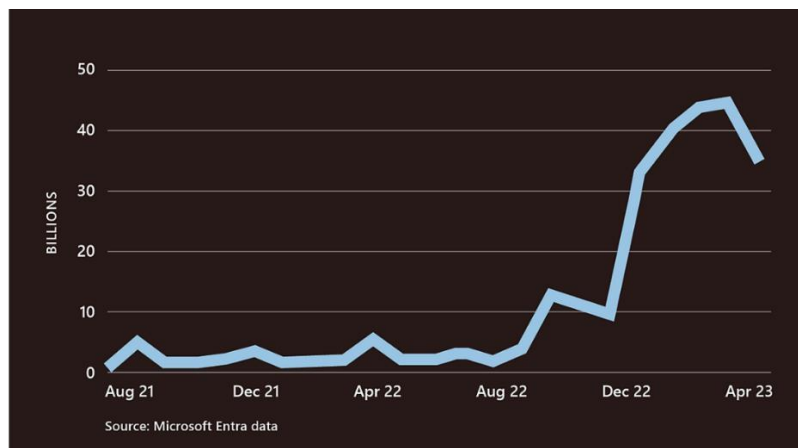
### **Povečanje človeško vodenih napadov z izsiljevalsko programsko opremo:**

Microsoft je zaznal več kot 200 % porast napadov z izsiljevalsko programsko opremo, pri katerih napadalci uporabljajo napredne tehnike, usmerjene predvsem proti manjšim podjetjem.



Slika 12: Pogled na področje izsiljevalskih napadov<sup>16</sup>

**Napadi, temelječi na geslih, so se povečali za desetkrat:** Število poskusov napadov na gesla je naraslo predvsem zaradi nezadostne uporabe MFA. Microsoft priporoča uporabo varnih poverilnic, kot so FIDO (Fast Identity Online) ključi.



Slika 13: Kako se področje groženj razvija<sup>17</sup>

**Povečanje napadov na poslovna e-poštna sporočila:** Napadi z zlorabo poslovnih e-poštnih računov so dosegli najvišjo stopnjo v zgodovini. Ti napadi postajajo vse bolj sofisticirani zaradi uporabe naprednih tehnik družbenega inženiringa.

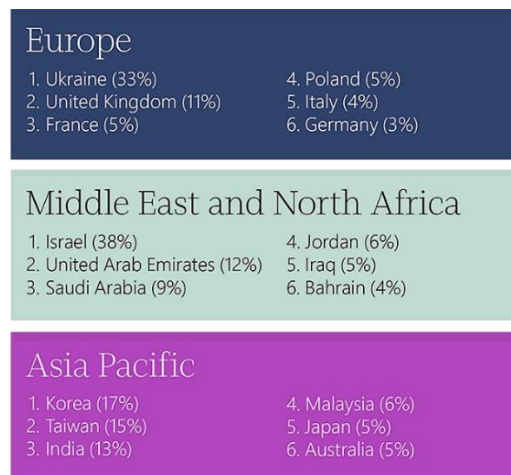
<sup>16</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_05\\_Human-operated-ransomware@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qit=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_05_Human-operated-ransomware@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qit=100&fmt=png-alpha&fit=constrain)

<sup>17</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_07\\_10x-more-password-attacks\\_v2@2x-1-1?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qit=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_07_10x-more-password-attacks_v2@2x-1-1?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qit=100&fmt=png-alpha&fit=constrain)



Slika 14: Število dnevni poskusov kompromisov poslovne e-pošte od aprila 2022 do aprila 2023 <sup>18</sup>

**Nacionalne državne grožnje so se razširile:** Državni napadalci so začeli ciljati na kritično infrastrukturo, izobraževalne ustanove in politične organizacije, v okviru širših geopolitičnih in vohunskih ciljev.



Slika 15: Najbolj ciljane države po regijah <sup>19</sup>

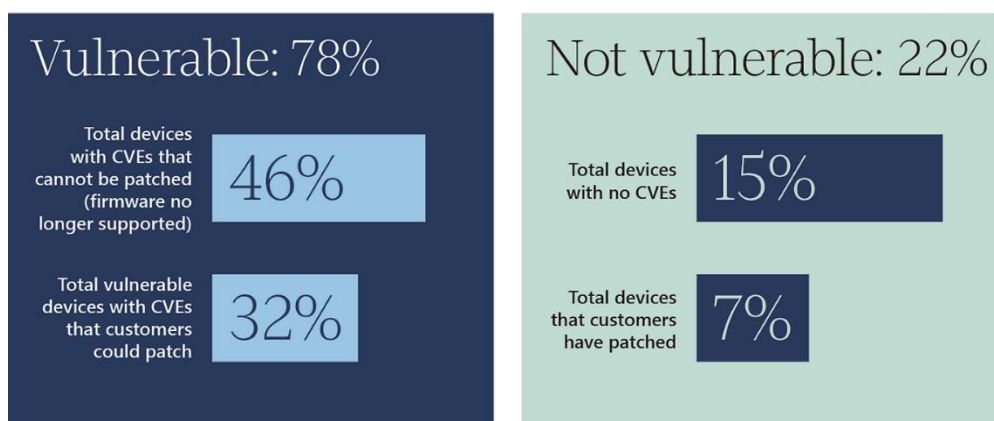
**Kombinacija kibernetških napadov in vplivnih operacij:** Državni napadalci zdaj pogosto izvajajo kibernetške napade skupaj z vplivnimi operacijami, da širijo propagando ali povzročijo socialne napetosti.

**Ogroženost naprav IoT in OT:** Napravam IoT (naprave z dostopom do interneta) in OT (največkrat naprave za upravljanje industrijskih procesov), ki so pogosto ranljive

<sup>18</sup> [https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_11\\_156k-daily-BEC-attempts@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_11_156k-daily-BEC-attempts@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

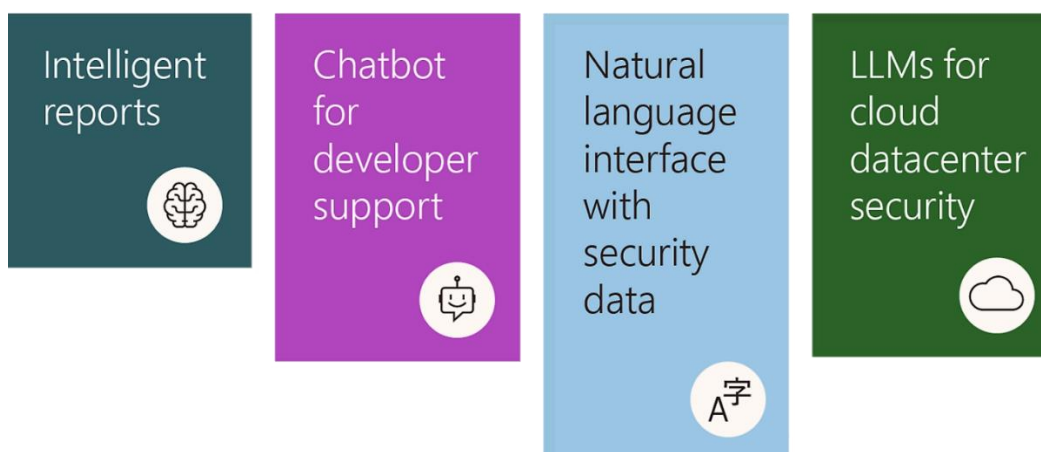
<sup>19</sup> [https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_01\\_Most-targeted-nations@2x-1?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_01_Most-targeted-nations@2x-1?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

zaradi zastarelih operacijskih sistemov in so tarče napadov Microsoft priporoča redno posodabljanje teh naprav in učinkovito spremljanje omrežij.



Slika 16: Delež ranljivih in neranljivih IoT naprav<sup>20</sup>

**Umetna inteligenca ima velik potencial za izboljšanje kibernetške varnosti:** UI lahko avtomatizira varnostne naloge, kar omogoča hitrejšo odkrivanje groženj in skrije vzorce napadov. LLM (veliki jezikovni modeli) so lahko v pomoč pri analizi groženj, odzivih na incidente ter izobraževanju.

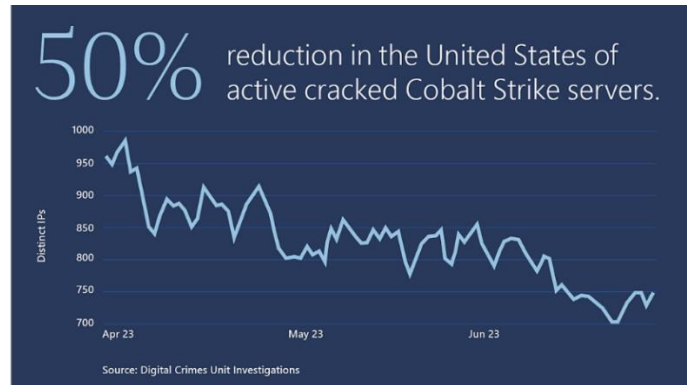


Slika 17: UI in veliki jezikovni modeli (LLM) bodo spremenili kibernetško varnost<sup>21</sup>

<sup>20</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_09\\_Device-vulnerabilities@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_09_Device-vulnerabilities@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

<sup>21</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_03\\_LLM-application-in-cyber@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_03_LLM-application-in-cyber@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

**Sodelovanje med javnim in zasebnim sektorjem je ključnega pomena:** Microsoft poudarja, da mora biti sodelovanje med vladnimi organizacijami, podjetji in raziskovalci ključni element za učinkovito bojevanje proti kibernetškim grožnjam.



Slika 18: Grafikon - 50-odstotno zmanjšanje vlomljenih strežnikov Cobalt Strike v ZDA <sup>22</sup>

**Pomanjkanje strokovnjakov za kibernetško varnost:** Zaradi naraščajočih groženj in vedno večje zapletenosti je nujno, da se poveča število usposobljenih strokovnjakov za kibernetško varnost. Microsoft se zavzema za izobraževanje in usposabljanje novih kadrov, vključno z uvajanjem programov za učenje umetne inteligence.



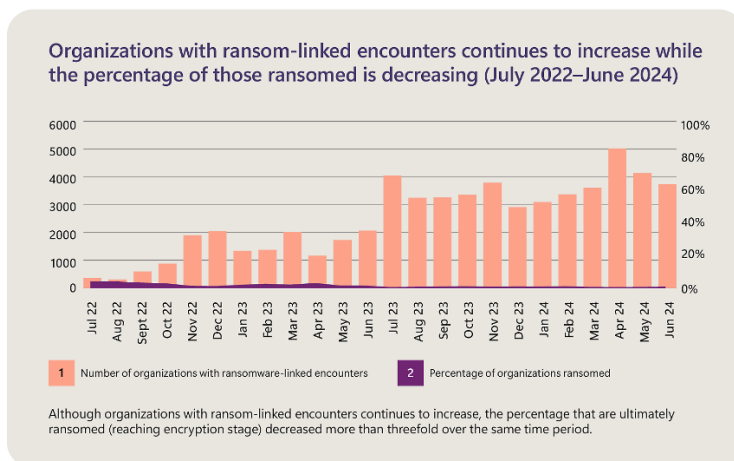
Slika 19: V zadnjem letu se je povpraševanje po strokovnjakih za kibernetško varnost povečalo za 35% <sup>23</sup>

<sup>22</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_08\\_Collaboration-takes-down@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_08_Collaboration-takes-down@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

<sup>23</sup>[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR\\_12\\_Cybersecurity-growth-map@2x?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/MDDR_12_Cybersecurity-growth-map@2x?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=686&qlt=100&fmt=png-alpha&fit=constrain)

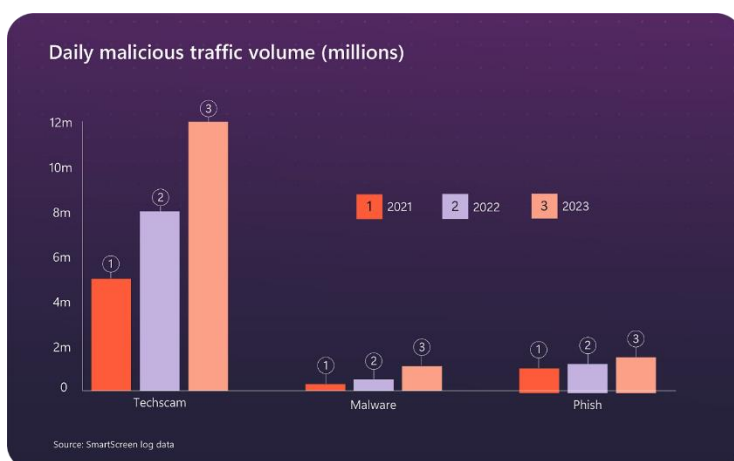
## Poročilo 2024

**3-kratni padec napadov v fazi izsiljevanja:** Kljub 2,75-kratnemu povečanju napadov, povezanih z izsiljevanjem, se je število napadov, ki so dosegli fazo izsiljevanja, zmanjšalo za trikrat zaradi samodejnih prekinitev napadov. Napadi pogosto izhajajo iz naprav brez ustreznega upravljanja, ki nimajo potrebne zaščite.



Slika 20: 3-kratno zmanjšanje napadov na stopnji odkupnine kljub 2,75-kratnemu povečanju števila srečanj<sup>24</sup>

**Povečanje števila tehnoloških prevar:** Napadi, kot so prevarantske podporne storitve, lažni kriptografski shemi in prevarantske brskalniške razširitve, so naraščali in postali večji problem kot zlonamerna programska oprema ali phishing.



Slika 21: Dnevni obseg zlonamernega prometa<sup>25</sup>

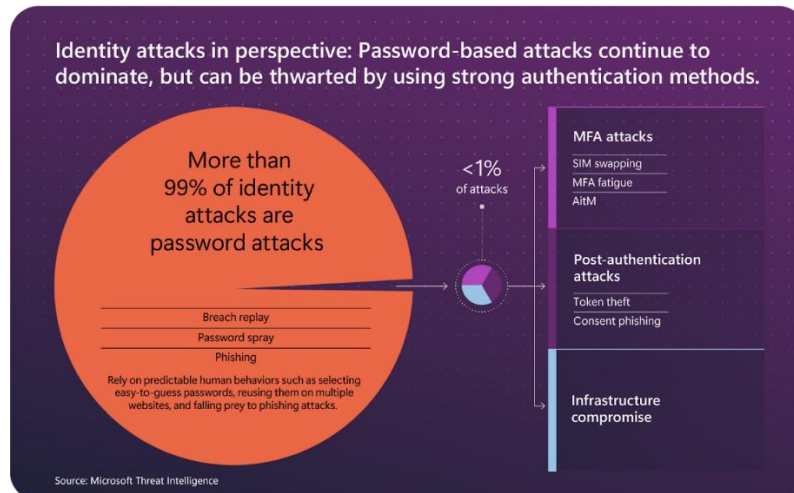
<sup>24</sup> [https://cdn-dynmedia-](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image1?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

[1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_Report\\_2024\\_Image1?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image1?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

<sup>25</sup> [https://cdn-dynmedia-](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_R)

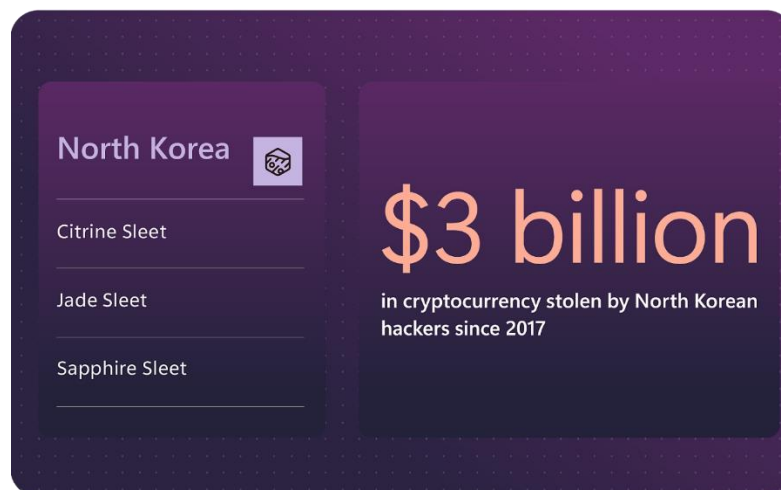
[1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_R](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_R)

**99 % napadov na identiteto temelji na geslih:** Napadalci še vedno izkoriščajo šibka in ponavljajoča se gesla, čeprav se povečuje uporaba več faktorske avtentikacije (MFA). Napadi vključujejo phishing (lažno predstavljanje) in krajo prijavnih podatkov.



Slika 22: Več kot 99 % napadov na identiteto so napadi z gesli <sup>26</sup>

**Nacionalne države in kibernetški kriminal:** Državni akterji so začeli uporabljati orodja in taktike kibernetških kriminalcev, vključno z ransomware (izsiljevalski virus) in krajo kriptovalut, kot je primer Severne Koreje, ki je od leta 2017 ukradla več kot 3 milijarde dolarjev v kriptovalutah.



Slika 23: Kriptovalute, ki so jih ukradli Severno Korejski hekerji <sup>27</sup>

[eport\\_2024\\_Image2?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image2?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

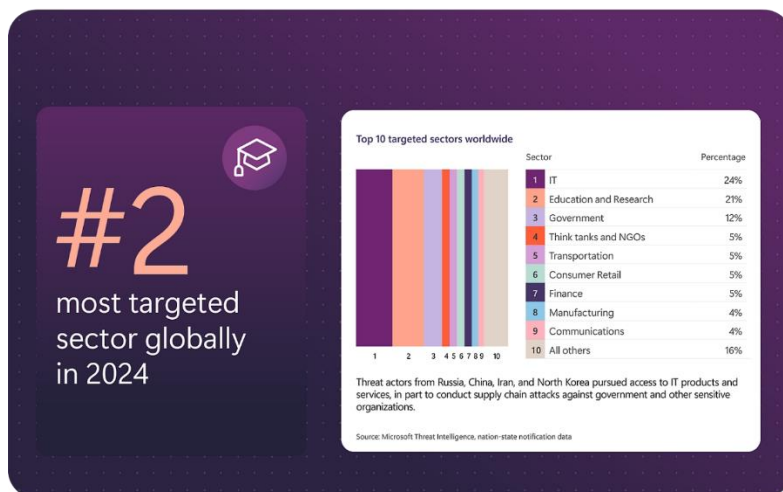
<sup>26</sup> [https://cdn-dynmedia-](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image3?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

[1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_Report\\_2024\\_Image3?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image3?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

<sup>27</sup> [https://cdn-dynmedia-](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_R)

[1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_R](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_R)




**Izobraževalni in raziskovalni sektor pod napadom:** V letu 2024<sup>28</sup> so bili izobraževalni in raziskovalni sektorji med najpogosteje ciljanimi s strani nacionalnih držav, ki uporabljajo napredne napadalne tehnike, kot je phishing (lažno predstavljanje) preko QR kod.



Slika 24: 10 najbolj napadenih sektorjev na svetu <sup>29</sup>

**Vpliv umetne inteligence na kibernetško varnost:** Državni akterji uporabljajo umetno inteligenco za okrepitev svojih kibernetških operacij in vplivne kampanje, kot je generiranje vsebine za manipulacijo medijev in volitev.

Adversarial use of AI in influence operations

Capability	China	Russia	Iran & proxies
Text	MEDIUM / LOW	MEDIUM / LOW	LOW
Image	HIGH	HIGH	MEDIUM / LOW
Audio/video	HIGH	HIGH	LOW
Example	May 2024: Bespoke Taizi Flood AI-generated cartoon 	June 2024: AI-generated audio of Elon Musk narrating fabricated documentary 	April 2024: Likely AI-generated video leading up to Iranian military operation 

Slika 25: Sposobnost sovražne uporabe umetne inteligence z namenom spletnega vpliva <sup>30</sup>

[https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_Report\\_2024\\_Image4?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image4?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

<sup>28</sup> Oktobra 2024 je bila žrtev obsežnega kibernetškega napada tudi Univerza v Mariboru

<sup>29</sup> [https://cdn-dynmedia-](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image5?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

[1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_Report\\_2024\\_Image5?resMode=sharp2&op\\_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_Report_2024_Image5?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=1600&hei=997&qlt=100&fmt=png-alpha&fit=constrain)

<sup>30</sup> [https://cdn-dynmedia-](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_R)

[1.microsoft.com/is/image/microsoftcorp/10\\_essential\\_insights\\_from\\_the\\_Microsoft\\_Digital\\_Defense\\_R](https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/10_essential_insights_from_the_Microsoft_Digital_Defense_R)

**Umetna inteligenca v obrambi: Red teaming:** Umetna inteligenca se uporablja za izboljšanje varnosti z metodo red teaminga, kjer se simulirajo napadi za iskanje ranljivosti. Ta pristop omogoča pravočasno prepoznavanje in odpravljanje tveganj.

**Iniciativa za varno prihodnost:** Microsoft je z Inicijativo za varno prihodnost odstranil milijone nezdružljivih aplikacij in neaktivnih najemnikov, s čimer je zmanjšal napadalne površine in povečal varnost.

**Hierarhija potrebščin kibernetške varnosti:** Poročilo ponuja strateški okvir za prednostno obravnavo varnostnih potrebščin, ki vključuje zaščito identitet, naprav, digitalnih sredstev in uporabe umetne inteligence za izboljšanje odzivanja na grožnje.

**Kolektivna obramba:** Sodelovanje med vlada, industrijami in podjetji je ključno za okrepitev kibernetške varnosti. Pobude, kot sta NATO-ov Defense Innovation Accelerator in Roundtable for AI, Security, and Ethics, poudarjajo pomen skupnih naporov v boju proti kibernetškim grožnjam.

### **3 RAZISKOVALNI DEL**

#### **3.1 METODE RAZISKOVANJA**

##### **3.1.1 Preučevanje literature**

Raziskovanje sem začel z zbiranjem literature s področja kibernetške varnosti in uporabe umetne inteligence pri zaščiti omrežij. Osredotočil sem se na strokovne članke, raziskovalna poročila in regulativne dokumente, ki obravnavajo to tematiko. Na podlagi teh virov sem oblikoval teoretični okvir svoje raziskovalne naloge. Pri izbiri literature sem se osredotočil na relevantne in zanesljive vire, ki neposredno prispevajo k razumevanju obravnavane problematike.

##### **3.1.2 Spletna anketa**

Da bi pridobil vpogled v razširjenost uporabe umetne inteligence v kibernetški varnosti v Sloveniji, sem v februarju 2025 izvedel spletno anketo med 150 slovenskimi podjetji in javnimi ustanovami. Vprašalnik, ki sem ga izdelal s pomočjo orodja Google Forms, je vseboval vprašanja zaprtega, odprtega, polodprtega in lestvičnega tipa. Anketni vprašalnik (Priloga 1) je dostopna na spletnem naslovu <https://forms.gle/fpuHGEX4MJoXE11X9>. Podatke, pridobljene z anketo, sem uporabil kot kvantitativno metodo raziskovanja.

#### **3.2 ANALIZA ANKETNEGA VPRAŠALNIKA**

##### **3.2.1 Analiza ankete**

V obdobju dveh tednov, ko je bila anketa odprta za odgovore, sem prejel 29 izpolnjenih vprašalnikov. V nadaljevanju bom predstavil rezultate raziskave, na podlagi katerih bom preveril veljavnost postavljenih hipotez. Pri predstavljanju rezultatov sem upošteval načela varovanja zasebnosti, zato bodo podatki prikazani v anonimizirani obliki, brez razkrivanja identitete sodelujočih organizacij ali posameznikov.

### 3.2.2. Vprašanja

#### 1. OSNOVNI PODATKI

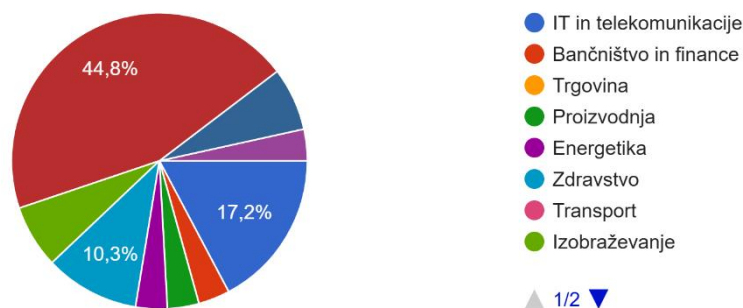
##### 1.1 Ime podjetja/ustanove

Anketni vprašalnik uvodoma vsebuje vprašanje glede imena podjetja/ustanove, vendar so za namen te raziskave odgovori anonimizirani in jih ne prikazujem. V nadaljevanju bom za vse organizacije, ne glede na njihovo organiziranost, uporabil izraz podjetje.

##### 1.2 V katero panogo spada vaše podjetje?

1.2. V katero panogo spada vaše podjetje?

29 odgovorov



Slika 26: Panoga podjetij

Vprašanje je zastavljeno z namenom pridobitve informacij o panogah, v katerih delujejo anketirana podjetja. To mi je omogočilo razvrščanje podjetij po sektorjih oziroma panogah in ugotavljanje stopnje razvitosti uporabe umetne inteligence v posameznih panogah. Na vprašanje je odgovorilo 29 anketirancev, ki prihajajo iz naslednjih panog:

**13** - Javna uprava (44,8 %)

**5** - IT in telekomunikacije (17,2 %)

**3** - Zdravstvo (10,3 %)

**2** - Izobraževanje (6,9 %)

**2** - Zavarovalništvo (6,9 %)

**1** - Bančništvo in finance (3,4 %)

**1** - Energetika (3,4 %)

**1** - Proizvodnja (3,4 %)

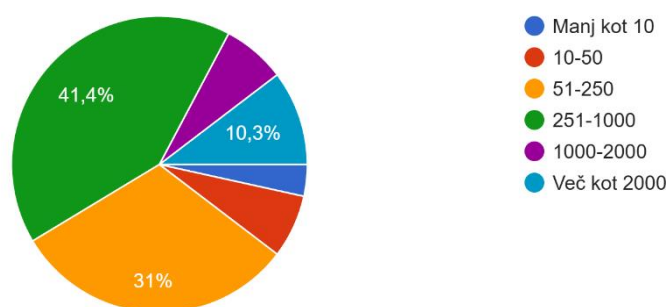
**1** - Regulacija (3,4 %)

Na podlagi prejetih odgovorov ugotavljam, da so bila na anketni vprašalnik bolj odzivna podjetja, ki so del javnega sektorja oz. ožji del javne uprave. Manj odzivna so bila zasebna podjetja, predvsem iz panoge transporta.

### 1.3 Koliko zaposlenih je v vašem podjetju?

1.3. Koliko zaposlenih je v vašem podjetju?

29 odgovorov



Slika 27: Število zaposlenih

To vprašanje sem zastavil z namenom pridobitve informacije o velikosti podjetij, ki sodelujejo v anketi. Na vprašanje je odgovorilo vseh 29 anketirancev, ki se po številu zaposlenih uvrščajo v naslednje kategorije:

**12** - 251–1000 zaposlenih

**2** - 1000–2000 zaposlenih

**9** - 51–251 zaposlenih

**2** - 10–50 zaposlenih

**3** - več kot 2000 zaposlenih

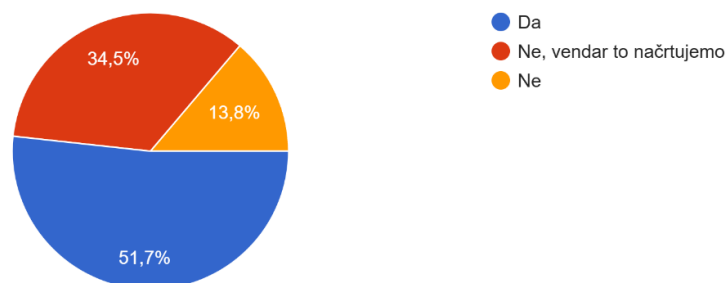
**1** - manj kot 10 zaposlenih

V raziskavi sodelujoča podjetja so večinoma srednje velika (do tisoč zaposlenih), kar nekaj pa je tudi velikih (nad tisoč zaposlenih). Podjetja z večjim številom zaposlenih so bolj izpostavljena tveganjem, povezanim s kibernetško varnostjo, in se pri zagotavljanju ustrezne ravni varnosti soočajo z bolj kompleksnimi izzivi.

## 1.4 Ali v vašem podjetju uporabljate umetno inteligenco?

1.4. Ali v vašem podjetju uporabljate umetno inteligenco?

29 odgovorov

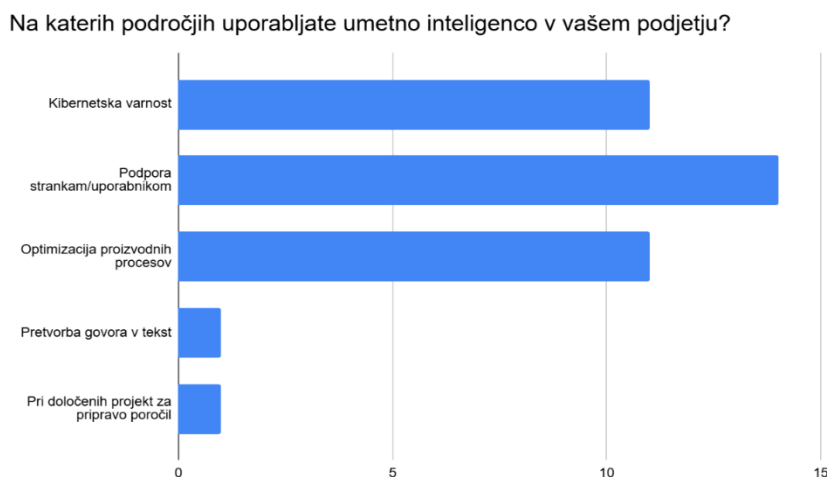


Slika 28: Uporaba umetne inteligence

Z zastavljenim vprašanjem sem želel pridobiti splošno informacijo o uporabi umetne inteligence med anketiranimi podjetji. Na vprašanje je odgovorilo vseh 29 anketirancev. Večina podjetij, natančneje 15 (51,7 %), že uporablja umetno inteligenco, medtem ko dobra tretjina, to je 10 (34,5 %), še ne uporablja, vendar načrtuje njeno uvedbo v prihodnosti. Le 4 podjetja (13,8 %) pa umetne inteligence ne uporabljajo in tudi ne načrtujejo njene uporabe v prihodnosti. Ugotavljam, da večina podjetij že uporablja umetno inteligenco, delež teh pa se bo v prihodnosti še povečeval, saj jih tretjina že načrtuje njeno uporabo v prihodnje. Z nadaljnjim razvojem umetne inteligence bo uporabna za vedno več stvari in bo tako tudi uporabljena v podjetjih različnih panog.

## 2. SPLOŠNA UPORABA UMETNE INTELIGENCE

### 2.1 Na katerih področjih uporabljate umetno inteligenco v vašem podjetju?



Slika 29: Področje uporabe umetne inteligence

To vprašanje sem zastavil z namenom boljšega razumevanja, na katerih področjih oz. pri katerih nalogah podjetja uporabljajo umetno inteligenco. Na vprašanje je odgovorilo vseh 29 anketirancev, pri čemer so se odgovori razporedili na naslednji način:

- **14 anketirancev** (48,3 %) uporablja umetno inteligenco za podporo strankam/uporabnikom;
- **11 anketirancev** (37,9 %) jo uporablja na področju kibernetške varnosti;
- **11 anketirancev** (37,9 %) jo uporablja za optimizacijo proizvodnih procesov;
- **7 anketirancev** (24,1 %) umetne inteligence ne uporablja ali pa niso želeli razkriti področij uporabe;
- **1 anketiranec** (3,4 %) jo uporablja za pretvorbo govora v besedilo;
- **1 anketiranec** (3,4 %) jo uporablja pri določenih projektih za pripravo poročil.

Ugotavljam, da podjetja umetno inteligenco najpogosteje uporabljajo v obliki t. i. "AI chatbotov", ki pomagajo uporabnikom pri preprostih vprašanjih. Ko ti ne morejo zagotoviti ustreznega odgovora, pogovor preusmerijo na človeške operaterje. Na ta

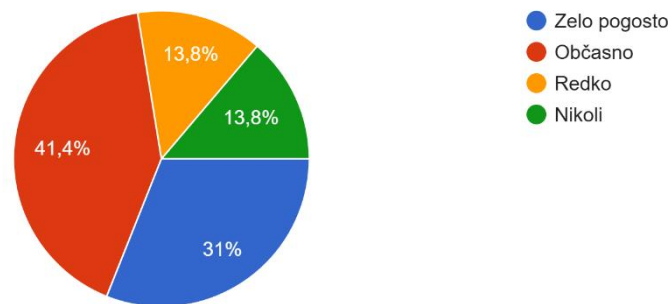
način podjetja prihranijo čas in stroške, saj potrebujejo manj zaposlenih v podpornih službah.

Pomembni področji uporabe umetne inteligence v podjetjih so tudi optimizacija proizvodnih procesov in kibernetška varnost, ki je osrednja tema te raziskave. To bo še posebej koristno pri analizi rezultatov v nadaljevanju.

## 2.2 Kako pogosto uporabljate umetno inteligenco pri vsakodnevnem delu?

2.2. Kako pogosto uporabljate umetno inteligenco pri vsakodnevnem delu?

29 odgovorov



Slika 30: Pogostost uporabe umetne inteligence

Vprašanje sem zastavil z namenom pridobitve informacije o pogostosti uporabe umetne inteligence med anketiranimi podjetji. Na vprašanje je odgovorilo vseh 29 anketirancev. Največ, 12 (41,4 %), umetno inteligenco uporablja občasno, 9 (31 %) zelo pogosto, 4 (13,8 %) redko, 4 (13,8 %) pa umetne inteligence ne uporablja nikoli.

Ugotavljam, da večina anketiranih podjetij umetno inteligenco uporablja vsaj občasno (41,4 %) ali zelo pogosto (31 %), kar kaže na njeno vse večjo vlogo v poslovnih procesih. Kljub temu pa jo 13,8 % podjetij uporablja le redko, enak delež (13,8 %) pa umetne inteligence sploh ne uporablja.

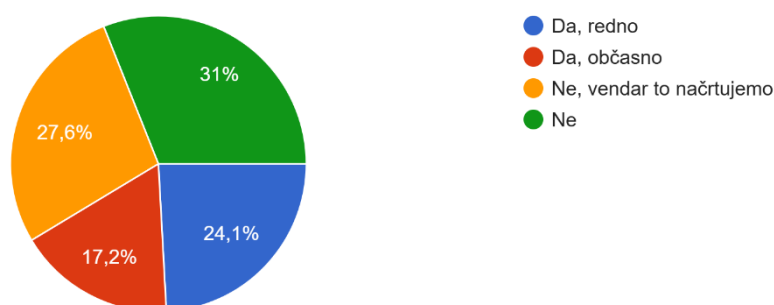
Ti rezultati nakazujejo, da se umetna inteligenca postopoma uveljavlja v poslovnem okolju, vendar nekatera podjetja še vedno oklevajo pri njeni uvedbi zaradi pomanjkanja virov, znanja ali nezadostne potrebe po avtomatizaciji in analitiki.

### 3. UPORABA UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI

#### 3.1 Ali v vašem podjetju uporabljate umetno inteligenco za zaščito pred kibernetškimi grožnjami?

3.1. Ali v vašem podjetju uporabljate umetno inteligenco za zaščito pred kibernetškimi grožnjami?

29 odgovorov



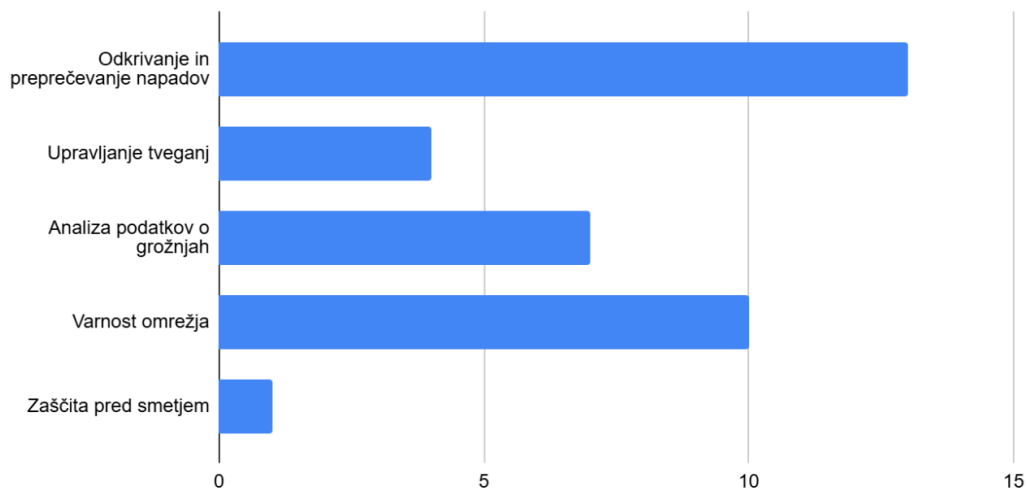
Slika 31: Uporaba umetne inteligence za zaščito pred kibernetškimi grožnjami

Vprašanje sem zastavil z namenom pridobiti informacije o uporabi umetne inteligence na področju kibernetške varnosti. Na vprašanje je odgovorilo vseh 29 anketirancev, od katerih jih 12 (41,3 %) uporablja umetno inteligenco, za kibernetško varnost jo 7 (24,1 %) uporablja pogosto, 5 (17,2 %) pa občasno. Na drugi strani 8 (27,6 %) podjetij umetno inteligenco na področju kibernetške varnosti namerava uporabljati v prihodnosti, 9 (31 %) pa umetne inteligence ne uporablja in je ne namerava niti v prihodnosti.

Ugotavljam, da umetno inteligenco na področju kibernetške varnosti uporablja več kot polovica podjetij, ki že uporabljajo UI. Čeprav je ta delež trenutno manjšinski v celotni populaciji anketiranih podjetij, rezultati kažejo na velik potencial za rast, saj 27,6 % podjetij načrtuje njeno uvedbo v prihodnosti. Kljub temu pa 31 % podjetij umetne inteligence na področju kibernetške varnosti ne uporablja in je tudi ne namerava, kar nakazuje na razlike v potrebah in pripravljenosti za uvajanje naprednih varnostnih rešitev.

### 3.2 Na katerih področjih kibernetške varnosti uporabljate umetno inteligenco?

Na katerih področjih kibernetške varnosti uporabljate umetno inteligenco?



Slika 32: Področja kibernetške varnosti kjer se uporablja umetna inteligenca

Vprašanje sem zastavil z namenom pridobiti informacije o uporabi umetne inteligence na različnih podpodročjih v okviru področja kibernetške varnosti. Na vprašanje je odgovorilo vseh 29 anketirancev, od katerih jo največ, 13 (44,8 %), uporablja za odkrivanje in preprečevanje napadov, 11 (37,9 %) je ne uporablja, 10 (34,5 %) jo uporablja za zagotavljanje varnosti omrežja, 7 (24,1 %) za analizo podatkov o grožnjah, 4 (13,8 %) za upravljanje tveganj in 1 (3,4 %) za zaščito pred smetjem.

Ugotavljam, da se umetna inteligenca v kibernetški varnosti najpogosteje uporablja za odkrivanje in preprečevanje napadov (44,8 %) ter zagotavljanje varnosti omrežja (34,5%). Prav tako jo relativno velik delež (24,1 %) uporablja za analizo podatkov o grožnjah, 13,8 % za upravljanje tveganj in 3,4 % za zaščito pred smetjem.

Kljub široki uporabi pa 37,9 % anketirancev umetne inteligence sploh ne uporablja na tem področju. To kaže, da nekatera podjetja še vedno zaupajo le tradicionalnim varnostnim rešitvam. Umetna inteligenca pa se vse bolj uveljavlja kot ključno orodje pri zgodnjem odkrivanju in preprečevanju kibernetških groženj.

### 3.3 Katere prednosti opažate pri uporabi umetne inteligence na področju kibernetške varnosti?



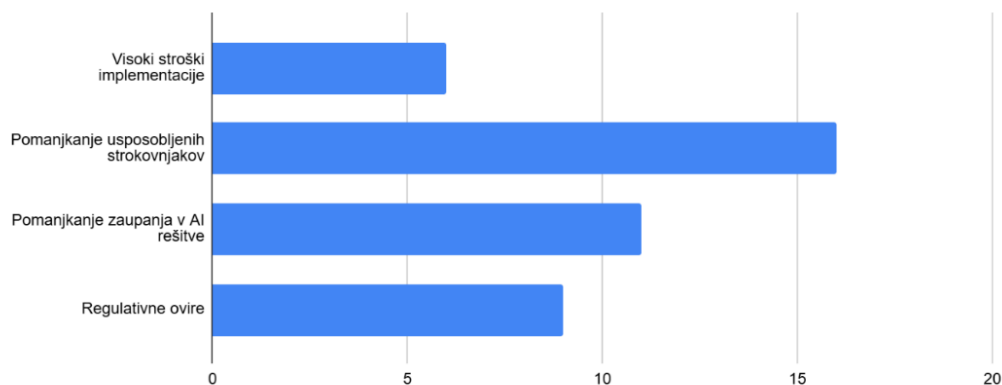
Slika 33: Prednosti uporabe umetne inteligence na področju kibernetške varnosti

Vprašanje sem zastavil z namenom pridobiti informacije o tem, katere prednosti opažajo podjetja z uporabo umetne inteligence na področju kibernetške varnosti. Na vprašanje, ki je omogočalo več odgovorov, je odgovorilo 21 anketirancev, od katerih 17 (81 %) opaža hitrejše odkrivanje groženj, 14 (66,7 %) večjo avtomatizacijo obrambnih sistemov, 11 (52,4 %) večjo natančnost pri prepoznavanju napadov, 6 (28,6 %) zmanjšanje stroškov varnosti, 1 (4,8 %) pa lažjo analizo in predstavitev podatkov.

Ugotavljam, da večina anketiranih podjetij opaža prednost v hitrejšem odkrivanju groženj (81 %) in večjo avtomatizacijo obrambnih sistemov (66,7 %) kot ključni prednosti uporabe umetne inteligence v kibernetški varnosti. Prav tako več kot polovica (52,4 %) podjetij poroča o večji natančnosti pri prepoznavanju napadov, medtem ko manjši delež anketirancev izpostavlja zmanjšanje stroškov varnosti (28,6 %) in lažjo analizo podatkov (4,8 %). Rezultati kažejo, da umetna inteligenca podjetjem predvsem izboljšuje učinkovitost in hitrost odziva na kibernetške grožnje.

### 3.4 Katere so glavne ovire za širšo uporabo umetne inteligence na področju kibernetške varnosti v vašem podjetju?

Katere so glavne ovire za širšo uporabo umetne inteligence na področju kibernetške varnosti v vašem podjetju?



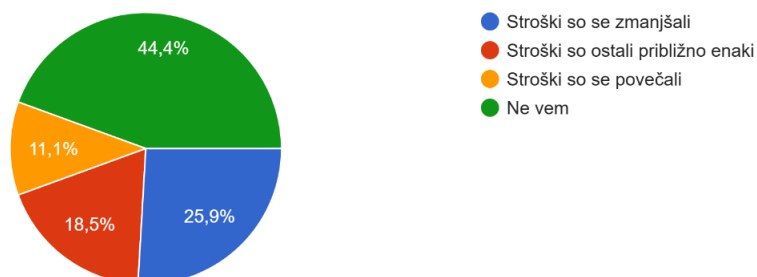
Slika 34: Glavne ovire za širšo uporabo umetne inteligence na področju kibernetške varnosti

Vprašanje sem zastavil z namenom pridobiti informacije o ovirah za širšo uporabo umetne inteligence na področju kibernetške varnosti. Na vprašanje je odgovorilo 23 anketirancev, od katerih jih 16 (69,6 %) vidi za glavno oviro pomanjkanje usposobljenih strokovnjakov, 12 (52,2 %) pomanjkanje zaupanja v rešitve UI, 9 (39,1 %) regulativne ovire, 6 (26,1 %) pa visoke stroške implementacije.

Ugotavljam, da večina anketiranih (69,6 %) kot največjo oviro za širšo uporabo umetne inteligence v kibernetški varnosti navaja pomanjkanje usposobljenih strokovnjakov. Poleg tega pomemben delež anketirancev (52,2 %) izpostavlja pomanjkanje zaupanja v rešitve UI, kar lahko ovira njihovo sprejemanje v podjetjih. Regulativne ovire (39,1 %) in visoki stroški implementacije (26,1 %) so prav tako pomembni izzivi, vendar se pojavljajo v manjšem obsegu. Rezultati kažejo, da so kljub potencialu umetne inteligence za izboljšanje kibernetške varnosti še vedno ključni izzivi na področju usposabljanja, zaupanja in regulacije.

### 3.5 Kakšen vpliv ima uporaba umetne inteligence na vaše stroške na področju kibernetške varnosti?

3.5 Kakšen vpliv ima uporaba umetne inteligence na vaše stroške na področju kibernetške varnosti?  
27 odgovorov



Slika 35: Vpliv uporabe umetne inteligence na področju kibernetške varnosti na stroške

Vprašanje sem zastavil z namenom pridobiti informacije o vplivu umetne inteligence na stroške podjetja na področju kibernetške varnosti. Na vprašanje je odgovorilo 27 anketirancev, od katerih jih 12 (44,4 %) ne ve, kakšna je bila sprememba v stroških, pri 7 (25,9 %) podjetjih so se stroški zmanjšali, pri 5 (18,5 %) so stroški ostali približno enaki, pri 3 (11,1 %) pa so se stroški povečali.

Presenetljiva ugotovitev je, da je relativno veliko anketirancev (44,4 %) ni vedelo, kako so se stroški spremenili ob uporabi umetne inteligence v kibernetški varnosti. Slednje pripisujem dejstvu, da so anketni vprašalnik izpolnjevale osebe, zadolžene za področje računalništva in informatike in ne vrhnji management, ki ima zagotovo pregled tudi nad stroški. Med tistimi, ki so lahko ocenili spremembo, je 25,9 % podjetij poročalo o zmanjšanju stroškov, 18,5 % jih je navedlo, da so stroški ostali približno enaki, 11,1 % pa je izpostavilo, da so se stroški povečali.

Če upoštevamo samo odgovore tistih, ki niso odgovorili z "ne vem", so rezultati naslednji:

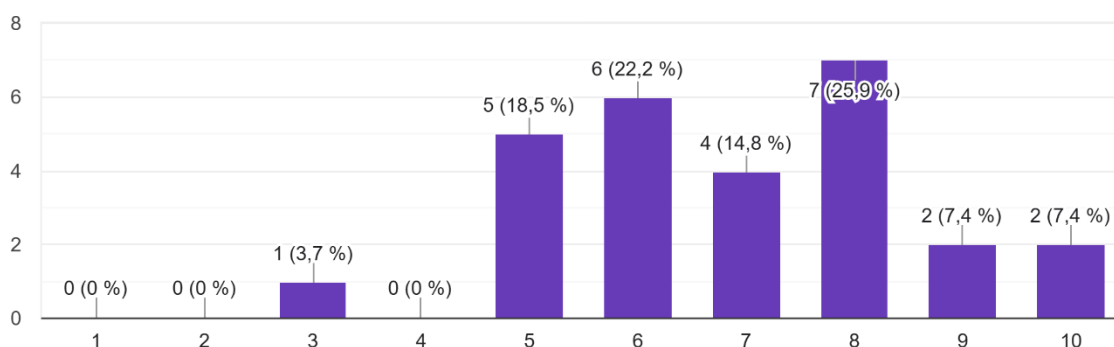
- 46,7 % podjetij je poročalo o zmanjšanju stroškov,
- 33,3 % podjetij je izjavilo, da so stroški ostali enaki,
- 20 % podjetij je izpostavilo povečanje stroškov.

Med podjetji, ki so podala odgovor, jih je stroške zmanjšalo kar 46,7 %. Stroški so se povečali pri 20 % podjetij, preostali pa so poročali o nespremenjenih stroških. To nakazuje, da umetna inteligenca v večini primerov prispeva k optimizaciji stroškov v kibernetški varnosti, vendar pa so pri nekaterih podjetjih lahko prisotni tudi dodatni stroški, povezani z implementacijo in vzdrževanjem rešitev UI.

### 3.6 Na lestvici od 1 do 10 ocenite, kako pomembna je uporaba umetne inteligence za izboljšanje kibernetške varnosti v vašem podjetju.

3.6. Na lestvici od 1 do 10 ocenite, kako pomembna je uporaba umetne inteligence za izboljšanje kibernetške varnosti v vašem podjetju? (1 = sploh ni pomembna, 10 = ključnega pomena)

27 odgovorov



Slika 36: Pomembnost uporabe umetne inteligence za izboljšanje kibernetške varnosti

Vprašanje sem zastavil z namenom pridobiti informacije o pomembnosti umetne inteligence za izboljšanje kibernetške varnosti. Na vprašanje je odgovorilo 27 anketirancev, od katerih jih je 7 (25,9 %) odgovorilo 8/10, na drugem mestu jih je 6 (22,2 %) odgovorilo s 6/10, 5 (18,5 %) s 5/10, 4 (14,8 %) s 7/10, po dva (7,4 %) z 9/10 in 10/10 ter 1 (3,7 %) anketiranec s 3/10.

Ugotavljam, da anketiranci ocenjujejo umetno inteligenco kot pomemben dejavnik za izboljšanje kibernetške varnosti, pri čemer jih večina (25,9 %) ocenjuje njen pomen z oceno 8/10. Povprečna ocena, ki so jo anketiranci dodelili umetni inteligenci, je 6,7/10, mediana pa je 7/10.

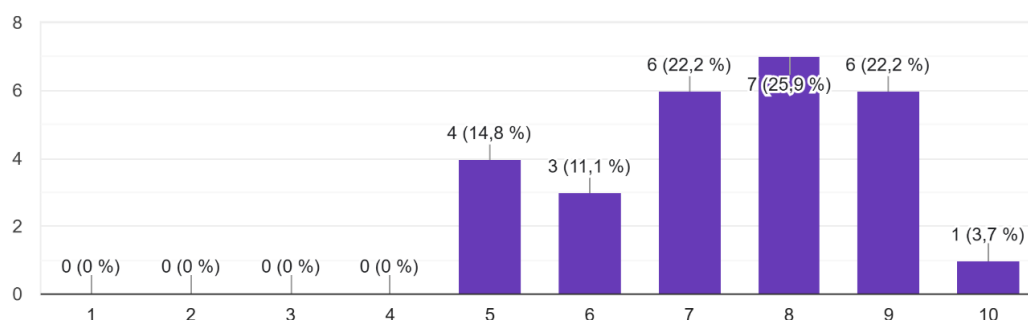
Nadalje ugotavljam, da so vsa podjetja, ki so odgovorila z oceno 5/10, med tistimi, ki umetne inteligence ne uporabljajo na področju kibernetške varnosti. Prav tako je podjetje, ki je odgovorilo s 3/10, eno izmed tistih, ki umetne inteligence sploh ne

uporablja. To nakazuje, da so podjetja, ki še niso implementirala umetne inteligence v svojo varnostno infrastrukturo, manj prepričana o njenem potencialu za izboljšanje kibernetške varnosti.

### 3.7 Kako ocenjujete učinkovitost umetne inteligence pri zaznavanju kibernetških groženj v primerjavi s tradicionalnimi metodami?

3.7. Kako ocenjujete učinkovitost umetne inteligence pri zaznavanju kibernetških groženj v primerjavi s tradicionalnimi metodami? (1 = manj učinkovita, 10 = veliko bolj učinkovita)

27 odgovorov



Slika 37: Ocena učinkovitosti UI v kibernetški varnosti v primerjavi s tradicionalnimi metodami

Vprašanje sem zastavil z namenom pridobiti informacije o učinkovitosti umetne inteligence pri zaznavanju kibernetških groženj v primerjavi s tradicionalnimi metodami. Na vprašanje je odgovorilo 27 anketirancev, od katerih jih je 7 (25,9 %) odgovorilo z 8/10, 6 (22,2 %) z 9/10, prav tako 6 (22,2 %) s 7/10, 4 (14,8 %) s 5/10, 3 (11,1 %) s 6/10 in 1 (3,7 %) z 10/10.

Ugotavljam, da anketiranci ocenjujejo umetno inteligenco kot zelo učinkovito pri zaznavanju kibernetških groženj v primerjavi s tradicionalnimi metodami. Povprečna ocena, ki so jo anketiranci dodelili umetni inteligenci pri zaznavanju groženj, je 7,3/10, mediana pa je 8/10.

Anketiranci, ki so odgovorili z oceno 5/10, ne uporabljajo umetne inteligence za kibernetško varnost, kar nakazuje, da je zaznavanje groženj z umetno inteligenco bolj cenjeno s strani podjetij, ki so jo že implementirala v svoje varnostne sisteme.

### **3.8 Katero področje kibernetške varnosti bi si po vašem mnenju lahko najbolj izboljšalo z uporabo umetne inteligence?**

Vprašanje sem zastavil z namenom pridobitve mnenja strokovnjakov o področjih kibernetške varnosti, ki bi jih lahko umetna inteligenca najbolj izboljšala. Na vprašanje je odgovorilo 12 anketirancev, ki so podali različne odgovore, saj je bilo vprašanje odprtega tipa. Tukaj je povzetek odgovorov:

- zaznavanje vdorov, proženje avtomatskih procedur, prijava incidentov na SI-CERT, obveščanje strank,
- omrežna varnost,
- zaščita pred napadi,
- Firewall,
- uporaba UI pri zaznavi napada na omrežje,
- področje zaznavanja in avtomatskega odzivanja na kibernetške napade,
- avtomatizacija trivialnih varnostnih pravil,
- avtomatizacija odgovorov na varnostne napade,
- napadi umetne inteligence na varnostne sisteme z umetno inteligenco,
- za ponavljajoče naloge, pripravo velikih količin vsebin, analizo in korelacijo podatkov,
- odzivnost, vidljivost,
- korelacija med incidenti, ki jih zazna orodje SIEM.

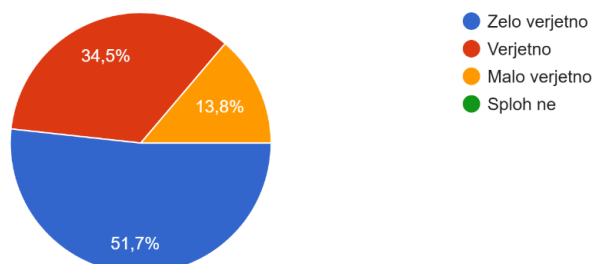
Iz odgovorov je razvidno, da anketiranci vidijo velik potencial umetne inteligence predvsem na področju zaznavanja in odzivanja na napade (npr. zaznavanje vdorov, omrežna varnost, avtomatizacija odgovorov na napade). Nekateri pa opozarjajo tudi na uporabo UI pri analizi podatkov in korelaciji incidentov. Pojavljajo se tudi mnenja, da bi UI lahko pomagala pri avtomatizaciji ponavljajočih nalog.

## 4. PRIHODNOST UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI

### 4.1 Ali menite, da bo umetna inteligenca v prihodnosti ključni element kibernetške varnosti?

4.1. Ali menite, da bo umetna inteligenca v prihodnosti ključni element kibernetške varnosti?

29 odgovorov



Slika 38: Pomembnost umetne inteligenca v kibernetški varnosti v prihodnosti

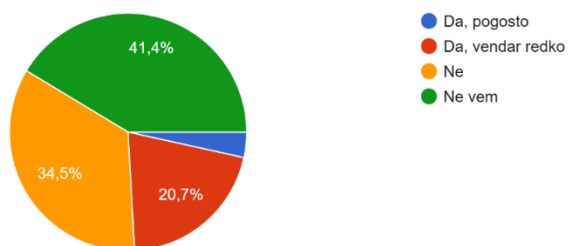
Vprašanje sem zastavil z namenom pridobiti mnenja o pomembnosti umetne inteligenca za področje kibernetške varnosti v prihodnosti. Na vprašanje je odgovorilo 29 anketirancev, od katerih jih 15 (51,7 %) meni, da bo umetna inteligenca v prihodnosti zelo verjetno ključni element kibernetške varnosti, 10 (34,5 %) verjetno, 4 (13,8 %) anketiranci pa so mnenja, da je to malo verjetno.

Ugotavljam, da večina anketirancev meni, da bo umetna inteligenca v prihodnosti ključni element kibernetške varnosti. Rezultati kažejo, da med podjetji obstaja široko prepričanje v pomembnost umetne inteligenca za prihodnost kibernetške varnosti.

### 4.2 Ali v vašem podjetju opažate porast napadov na vaše strežnike, ki vključujejo uporabo umetne inteligenca?

4.2. Ali v vašem podjetju opažate porast napadov na vaše strežnike, ki vključujejo uporabo umetne inteligenca?

29 odgovorov



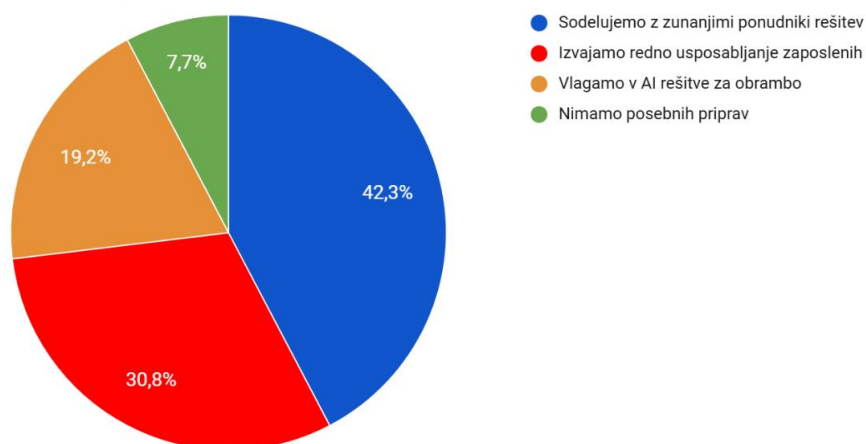
Slika 39: Porast napadov na strežnike, ki vključujejo uporabo umetne inteligenca

Vprašanje sem zastavil z namenom pridobiti informacije o porastu napadov na strežnike podjetij, ki vključujejo uporabo umetne inteligence. Na vprašanje je odgovorilo 29 anketirancev, od katerih jih 12 (41,4 %) ne ve, ali opažajo porast napadov na strežnike, ki vključujejo uporabo umetne inteligence, 10 (34,5 %) porasta ne opaža, 6 (20,7 %) opaža porast, vendar redko, 1 (3,4 %) pa porast opaža pogosto.

Ugotavljam, da večina anketirancev ni opazila jasnega porasta napadov na strežnike podjetij, ki vključujejo uporabo umetne inteligence. Rezultati nakazujejo, da uporaba umetne inteligence v napadih na strežnike podjetij še ni postala širše opažena grožnja.

#### 4.3 Kako se vaše podjetje pripravlja na obrambo pred napadi, ki vključujejo umetno inteligenco?

Kako se vaše podjetje pripravlja na obrambo pred napadi, ki vključujejo umetno inteligenco?



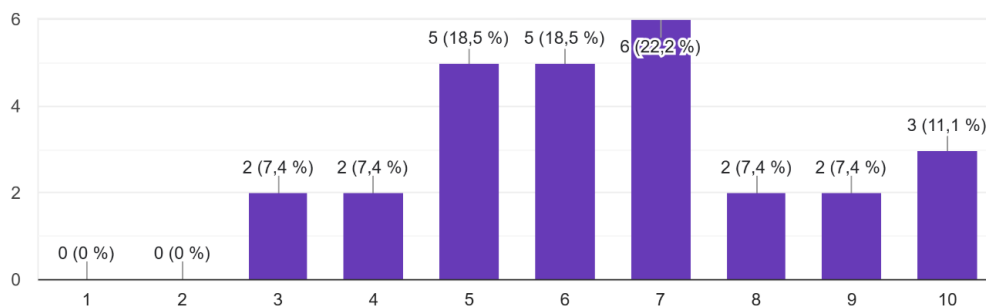
Slika 40: Priprave na obrambo pred napadi, ki vključujejo umetno inteligenco

Vprašanje sem zastavil z namenom pridobiti informacije o pripravah različnih podjetij na obrambo pred napadi, ki vključujejo umetno inteligenco. Na vprašanje je odgovorilo 26 anketirancev, od katerih jih 11 (42,3 %) sodeluje z zunanjimi ponudniki rešitev, 8 (30,8 %) redno usposablja zaposlene, 5 (19,2 %) vlaga v rešitve UI za obrambo, 2 (7,7 %) pa nimata posebnih priprav.

Ugotavljam, da se podjetja na različne načine pripravljajo na obrambo pred napadi, ki vključujejo umetno inteligenco. Podjetja vse bolj prepoznavajo potrebo po sodelovanju z zunanjimi strokovnjaki in izobraževanju zaposlenih, vendar še vedno obstajajo takšna, ki nimajo specifičnih priprav za tovrstne napade, slednja so predvsem manjša.

#### 4.4 Na lestvici od 1 do 10 ocenite, kako pripravljeno je vaše podjetje na obrambo pred kibernetškimi napadi, ki vključujejo uporabo umetne inteligence.

4.4. Na lestvici od 1 do 10 ocenite, kako pripravljeno je vaše podjetje na obrambo pred kibernetškimi napadi, ki vključujejo uporabo umetne inteligence. (...sploh ni pripravljeno, 10 = popolnoma pripravljeno)  
27 odgovorov



Slika 41: Ocena pripravljenosti pred kibernetškimi napadi, ki vključujejo uporabo UI

Vprašanje sem zastavil z namenom pridobiti informacije o pripravljenosti različnih podjetij na obrambo pred napadi, ki vključujejo umetno inteligenco. Na vprašanje je odgovorilo 27 anketirancev, od katerih je 6 (22,2 %) ocenilo svojo pripravljenost s 7/10, 5 (18,5 %) anketirancev s 6/10 in 5/10, 3 (11,1 %) anketiranci z 10/10, po dva anketiranci (7,4 %) pa z 9/10, 8/10, 4/10 in 3/10.

Ugotavljam, da anketiranci različno ocenjujejo pripravljenost svojih podjetij na obrambo pred napadi, ki vključujejo umetno inteligenco. Povprečna ocena pripravljenosti je 6,1/10, mediana pa 6/10. Rezultati kažejo, da večina podjetij ocenjuje, da so delno ali srednje pripravljene, le manjši delež pa ocenjuje svojo pripravljenost kot zelo visoko.

#### 4.5 Kakšno vlogo pričakujete, da bo umetna inteligenca igrala pri zagotavljanju kibernetške varnosti v naslednjih petih letih?

Vprašanje sem zastavil z namenom pridobiti mnenja strokovnjakov o vlogi umetne inteligence pri zagotavljanju kibernetške varnosti v naslednjih petih letih. Na vprašanje je odgovorilo 15 anketirancev, ki so podali različne, a hkrati podobne odgovore, saj je bilo vprašanje odprtega tipa. Odgovori so predstavljeni v nadaljevanju:

- Najbrž bo zelo velika vloga.
- Zelo veliko.

- Zaznavanje in preprečevanje vdorov, dnevni pregled varnosti sistema, predlaganje in kasneje že implementacija rešitev.
- Veliko procesov, ki jih sedaj opravljamo ročno, bo avtomatizirano.
- Veliko vlogo, uporabljali bomo vsak dan na vseh področjih.
- Vedno večjo.
- Ključno.
- Veliko, saj bo opravljala ponavljajoče postopke in hitreje prepoznavala ter povezovala varnostne dogodke.
- Visoko.
- Prepoznavanje kibernetških napadov in avtomatski odgovor nanje.
- Ključno.
- Ne veliko.
- Največ v smislu analize podatkov in prepoznavne vzorcev.
- V prihodnosti bo umetna inteligenca igrala eno izmed ključnih vlog.
- UI bo analizirala in avtomatizirano ukrepala na 80 % zaznanih incidentov.

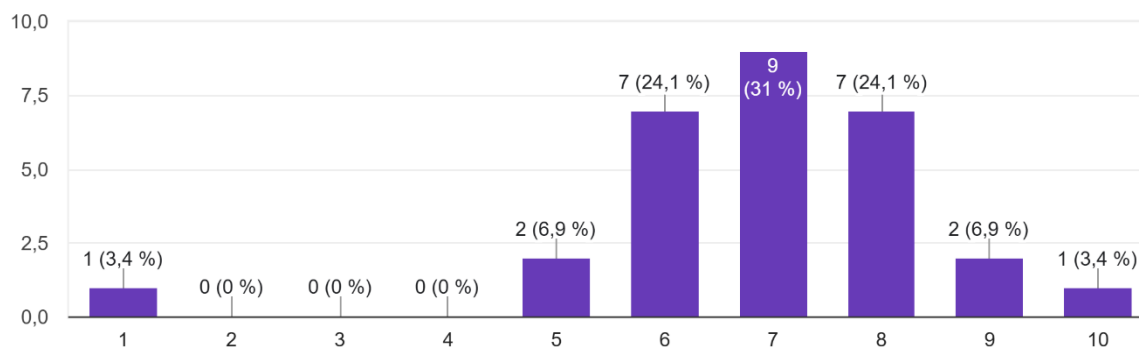
Iz odgovorov je razvidno, da večina anketirancev v prihodnosti pričakuje veliko vlogo umetne inteligence v kibernetški varnosti. Ključni poudarki vključujejo avtomatizacijo procesov, zaznavanje in preprečevanje vdorov ter analizo podatkov za prepoznavanje vzorcev in hitrejši odziv na incidente. Več odgovorov izpostavlja, da bo umetna inteligenca postala vsakodnevno uporabljeno orodje v kibernetški varnosti, nekateri pa menijo, da bo igrala celo ključno vlogo. Poleg teh pa obstaja tudi manjšinsko prepričanje, da umetna inteligenca v kibernetški varnosti v prihodnosti ne bo igrala velike vloge.

## 5. DODATNA VPRAŠANJA

### 5.1 Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Stroški implementacije

5.1. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Stroški implementacije

29 odgovorov



Slika 42: Ocena pomembnosti stroška implementacije na uvedbo umetne inteligence

Vprašanje sem zastavil z namenom pridobiti informacije o tem, kako podjetja ocenjujejo vpliv stroškov implementacije na uvedbo umetne inteligence pri njih. Na vprašanje je odgovorilo 29 anketirancev, od katerih jih 9 (31 %) ocenjuje s 7/10, 7 (24,1 %) z 8/10 in 6/10, 2 (6,9 %) z 9/10 in 5/10 ter po 1 (3,4 %) z 10/10 in 1/10.

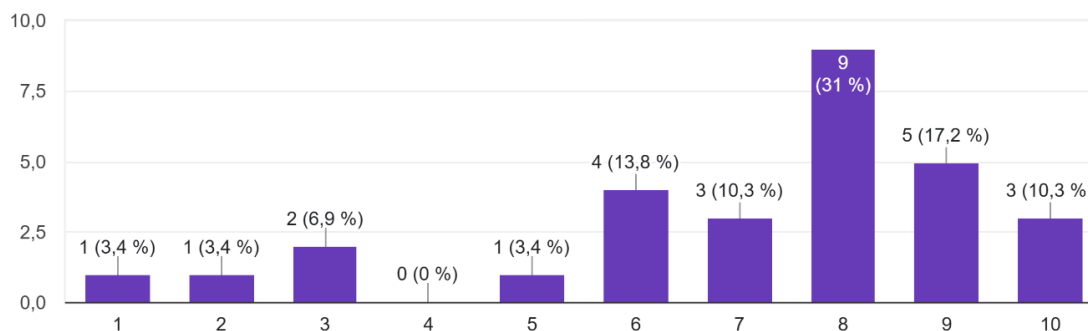
Ugotavljam, da anketiranci ocenjujejo stroške implementacije kot pomemben dejavnik pri uvedbi umetne inteligence v podjetjih. Povprečna ocena vpliva stroškov je 7,0/10, mediana pa 7/10.

Rezultati kažejo, da večina podjetij ocenjuje stroške kot srednje do visoko pomembne, pri čemer prevladujejo ocene med 6 in 8.

## 5.2 Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Razpoložljivost strokovnjakov

5.2. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Razpoložljivost strokovnjakov

29 odgovorov



Slika 43: Ocena pomembnosti razpoložljivosti strokovnjakov na uvedbo umetne inteligence

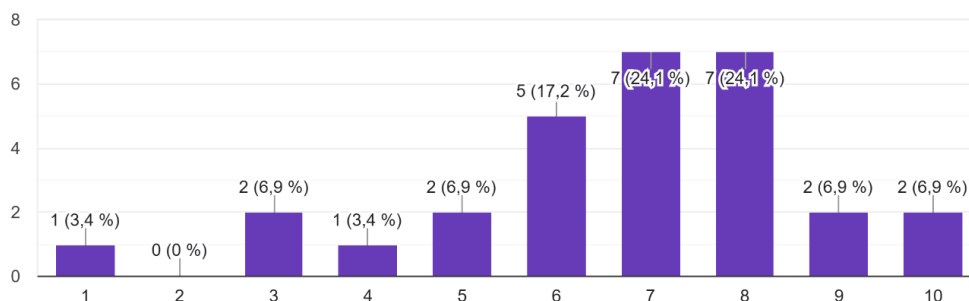
Vprašanje sem zastavil z namenom pridobitve informacije o tem, kako podjetja ocenjujejo vpliv razpoložljivosti strokovnjakov na uvedbo umetne inteligence pri njih. Na vprašanje je odgovorilo 29 anketirancev, od katerih jih 9 (31 %) ocenjuje ta dejavnik z 8/10, 5 (17,2 %) z 9/10, 4 (13,8 %) s 6/10, 3 (10,3 %) z 10/10 in 7/10, 2 (6,9 %) s 3/10 in po 1 (3,4 %) s 5/10, 2/10 in 1/10.

Ugotavljam, da podjetja različno ocenjujejo vpliv razpoložljivosti strokovnjakov na uvedbo umetne inteligence, vendar večina meni, da gre za pomemben dejavnik. Povprečna ocena vpliva je 7,1/10, mediana pa 8/10.

Rezultati kažejo, da se številna podjetja soočajo s pomanjkanjem strokovnjakov, kar lahko upočasni implementacijo umetne inteligence.

### 5.3 Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Zaupanje v tehnologijo

5.3. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Zaupanje v tehnologijo  
29 odgovorov



Slika 44: Ocena pomembnosti zaupanja v tehnologijo na uvedbo umetne inteligence

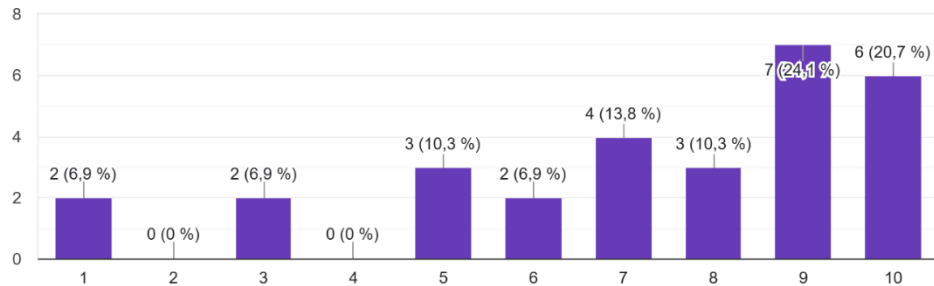
Vprašanje sem zastavil z namenom pridobiti informacije o tem, kako podjetja ocenjujejo vpliv zaupanja v tehnologijo na uvedbo umetne inteligence pri njih. Na vprašanje je odgovorilo 29 anketirancev, od katerih jih 7 (24,1 %) ocenjuje ta dejavnik z 8/10 in 7/10, 5 (17,2 %) s 6/10, 2 (6,9 %) z 10/10, 9/10, 5/10 in 3/10 ter po 1 (3,4 %) s 4/10 in 1/10.

Ugotavljam, da anketiranci zmerno zaupajo umetni inteligenci pri njeni uvedbi v podjetjih. Povprečna ocena zaupanja je 6,8/10, mediana pa 7/10.

Rezultati kažejo, da se večina podjetij nagiba k previdnemu sprejemanju umetne inteligence, pri čemer obstajajo tako njeni podporniki kot skeptiki.

## 5.4 Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Podpora vodstva

5.4. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: Podpora vodstva  
29 odgovorov



Slika 45: Ocena pomembnosti podpore vodstva na uvedbo umetne inteligence

Vprašanje sem zastavil z namenom pridobiti informacije o tem, kako podjetja ocenjujejo vpliv podpore vodstva na uvedbo umetne inteligence pri njih. Na vprašanje je odgovorilo 29 anketirancev, od katerih jih 7 (24,1 %) ocenjuje ta dejavnik z 9/10, 6 (20,7 %) z 10/10, 4 (13,8 %) s 7/10, 3 (10,3 %) z 8/10 in 5/10 ter po 2 (6,9 %) s 6/10, 3/10 in 1/10.

Ugotavljam, da podjetja večinoma ocenjujejo podporo vodstva kot pomemben dejavnik pri uvedbi umetne inteligence. Povprečna ocena vpliva podpore vodstva je 7,5/10, mediana pa 8/10.

Rezultati kažejo, da imajo podjetja z močnejšo podporo vodstva večjo verjetnost uspešne implementacije umetne inteligence, medtem ko pomanjkanje podpore lahko predstavlja oviro pri njenem uvajanju.

## 4 RAZPRAVA

Umetna inteligenca v današnjem času postaja ali pa je na nekaterih področjih že ključen del našega življenja. Uporabljamo jo za pomoč pri delu, podporo strankam in uporabnikom, kibernetško varnost, optimizacijo proizvodnih procesov in še na številnih drugih področjih. Kibernetška varnost je v času pospešene in vseprisotne digitalizacije postala ena izmed najpomembnejših dejavnosti za posameznike in organizacije. Hekerji nenehno razvijajo nove načine za obvladovanje sistemov in pridobivanje občutljivih informacij, zato je nujno, da zaščitimo naše digitalne vire z naprednimi rešitvami. Ena izmed najpomembnejših inovacij v tej smeri je uporaba umetne inteligence, ki omogoča napredne in dinamične metode zaščite. Slednja se v Sloveniji že uporablja, vendar zaenkrat še v manjšem obsegu. Pri teh, ki jo uporabljajo, se opaža hitrejša zaznava groženj, avtomatizacija obrambnih sistemov, večja natančnost pri prepoznavi groženj ter pri nekaterih tudi zmanjšanje stroškov. Glavna težava, s katero se podjetja srečujejo, je običajno pomanjkanje usposobljenih strokovnjakov, nekatera pa v UI rešitve preprosto ne zaupajo.

Pred pričetkom raziskovanja sem si zastavil sedem hipotez, ki sem jih s pomočjo izvedene raziskave potrdil oz. ovrgel. Rezultati za vsako od postavljenih hipotez so predstavljeni v nadaljevanju.

**Hipoteza 1:** Večina podjetij v Sloveniji že uporablja umetno inteligenco.

### ✓ **Potrjena**

To hipotezo sem potrdil, saj 51,7 % anketiranih podjetij že uporablja umetno inteligenco, hkrati pa jo v prihodnosti namerava uporabljati še dodatnih 34,5 % anketiranih podjetij. To kaže na hitro prilagajanje slovenskega gospodarstva na novosti na trgu. Zgodovina kaže, da so najbolj uspešni tisti, ki se znajo najbolje prilagoditi razmeram. Ugotovil sem tudi, da je ključnega pomena, da podjetja ne samo investirajo v tehnologijo, ampak tudi vlagajo v usposabljanje svojih zaposlenih, da bodo le tako lahko v polnosti izkoristili potencial umetne inteligence za izboljšanje kibernetške varnosti. Poleg tega se morajo osredotočiti tudi na razvoj etičnih smernic za uporabo umetne inteligence, da bi preprečili morebitno zlorabo tehnologije.

**Hipoteza 2:** Podjetja za kibernetško varnost v Sloveniji že uporabljajo umetno inteligenco, vendar v omejenem obsegu.

✓ **Potrjena**

To hipotezo sem potrdil, saj 41,3 % anketiranih podjetij že uporablja umetno inteligenco za kibernetško varnost, kar ni večinski delež, kaže pa na njeno uporabo v omejenem, a vseeno relativno velikem obsegu. Tako visok odstotek me je nekoliko presenetil, saj sem pričakoval, da se bo umetna inteligenca na tem področju uporabljala v manjšem obsegu zaradi relativne nerazvitosti Slovenije v primerjavi s zahodnoevropskimi državami in ZDA, kjer je slednja širše uporabljena. Poleg tega kar 27,6 % podjetij namerava uporabljati umetno inteligenco za kibernetško varnost v prihodnosti, kar kaže na ne tako velik zaostanek slovenskega gospodarstva v primerjavi s tujim na področju uporabe umetne inteligence.

**Hipoteza 3:** Večina slovenskih podjetij meni, da umetna inteligenca predstavlja velik potencial za izboljšanje kibernetške varnosti.

✓ **Potrjena**

To hipotezo sem potrdil, saj 51,7 % anketiranih podjetij meni, da bo umetna inteligenca v prihodnosti zelo verjetno ključen element kibernetške varnosti, 34,5 % anketiranih podjetij pa, da bo verjetno ključen element. Nobeno podjetje se ni opredelilo s »sploh ne«, 13,8 % pa se jih je z »malo verjetno«, kar nakazuje na močno prepričanje o velikem potencialu umetne inteligence v kibernetški varnosti. Rezultat me je malo presenetil, saj nisem pričakoval, da bo tako veliko podjetij videlo velik potencial v UI. Menil sem, da bo več podjetij izkazalo nezaupanje v umetno inteligenco tudi v prihodnosti.

**Hipoteza 4:** Glavna ovira za širšo uporabo umetne inteligence v kibernetški varnosti pri slovenskih podjetjih so visoki stroški implementacije in pomanjkanje strokovnjakov.

### ✓ **Potrjena**

To hipotezo sem potrdil saj 69,6 % anketiranih podjetij ovira pomanjkanje strokovnjakov pri širši uporabi umetne inteligence v kibernetški varnosti, 26,1 % pa visoki stroški implementacije. Rezultat je bil malo drugačen od pričakovanega, saj so med anketiranimi podjetji večja ovira kot visok strošek implementacije nezaupanje v umetno inteligenco in regulativne ovire. Te ugotovitve kažejo, da so kljub visokim stroškom za implementacijo, podjetja bolj zaskrbljena zaradi nezaupanja v umetno inteligenco in regulativnih ovir. To nakazuje, da podjetja potrebujejo več izobraževanja in jasnejše smernice, da bi povečala zaupanje v UI ter zmanjšala strah pred morebitnimi pravnimi in etičnimi težavami. Da bi omogočili širšo uporabo umetne inteligence v kibernetški varnosti, bi morali ustvariti ustrezno zakonodajo in povečati ozaveščenost o prednostih UI.

**Hipoteza 5:** Podjetja, ki uporabljajo umetno inteligenco, dosegajo hitrejše in natančnejše odkrivanje kibernetških groženj.

### ✓ **Potrjena**

To hipotezo sem potrdil, saj so prav vsa podjetja, ki umetno inteligenco uporabljajo za kibernetško varnost, ocenila njeno učinkovitost kot boljšo v primerjavi s tradicionalnimi metodami. Takšna enotnost odgovorov me ni presenetila, saj je logično, da bi podjetja v nasprotnem primeru uporabo umetne inteligence opustila. Umetna inteligenca namreč omogoča hitrejše odkrivanje in obvladovanje groženj, kar je ključnega pomena v svetu, kjer se kibernetški napadi stalno razvijajo. Povečanje učinkovitosti v boju proti napadom je zato odločilen dejavnik za vse večjo uporabo UI v tej panogi.

**Hipoteza 6:** Podjetja v Sloveniji se soočajo z večjimi izzivi pri obrambi pred napadi, ki uporabljajo umetno inteligenco zaradi njene naprednosti.

### × **Ovržena**

To hipotezo sem ovrzel, saj okoli 60 % podjetij niti ne opaža napadov, ki uporabljajo umetno inteligenco. Od podjetij, ki zaznavajo napade s pomočjo UI, kar 85 % podjetij takšne napade zaznava le redko. To kaže, da napadi, ki uporabljajo umetno

inteligenco, še niso tako pogosti in da podjetja še nimajo večjih težav s tem. Večina podjetij ocenjuje, da so pripravljeni na takšne napade, 15 % pa ocenjuje, da na tovrstne napade niso pripravljeni. Ta rezultat me ni presenetil, saj sem pričakoval, da takšni napadi, ki vključujejo umetno inteligenca, pri nas še niso dovolj razširjeni, da bi podjetja na njih naletela v večji meri. Povsem mogoče pa je tudi, da so napadi s pomočjo umetne inteligence usmerjeni v podjetja, ki sodijo v t. i. kritično infrastrukturo, ki pa na anketni vprašalnik večinoma niso podala odgovorov.

**Hipoteza 7:** Podjetja v Sloveniji vlagajo v UI rešitve in izvajajo redna usposabljanja zaposlenih.

✓ **Potrjena**

To hipotezo sem potrdil, saj se okoli 30 % podjetij na kibernetike grožnje pripravlja z rednim usposabljanjem zaposlenih, okoli 20 % pa vlaga v UI rešitve. Približno 40 % podjetij, predvsem manjših, pa sodeluje z zunanjimi ponudniki. Po mojem mnenju je takšen pristop razumljiv, saj podjetja vse bolj prepoznavajo pomen usposabljanja svojih zaposlenih in vlaganja v napredne tehnologije, kot je umetna inteligenca. Kljub temu pa se večja podjetja zaradi varnosti bolj zanašajo na notranje IT službe, medtem ko manjša podjetja iščejo zunanje strokovnjake za obvladovanje teh zahtevnih nalog.

## 5 ZAKLJUČEK

Raziskava je pokazala pomembno rast zavedanja in implementacije naprednih tehnologij v slovenskih podjetjih. Umetna inteligenca postaja ključna v kibernetški obrambi, saj omogoča hitrejšo analizo podatkov, zaznavanje anomalij in preprečevanje napadov. Podjetja prepoznavajo njen potencial, vendar še vedno obstajajo izzivi pri njeni širši implementaciji in prilagoditvi podjetij za učinkovito uporabo teh tehnologij. Eden ključnih izzivov, s katerimi se podjetja soočajo pri implementaciji umetne inteligence v kibernetško varnost, je pomanjkanje usposobljenih, strokovnih kadrov. Umetna inteligenca zahteva specifično znanje in usposobljenost, zato se podjetja pogosto soočajo s težavami pri iskanju primernih kadrov, ki bi jih lahko izobrazili za učinkovito uporabo teh naprednih rešitev. Takšnega kadra žal v Sloveniji primanjkuje. To pomeni, da je potrebna naložba tako v izobraževanje obstoječih kadrov kot v privabljanje novih strokovnjakov. Poleg tega se podjetja soočajo z izzivi pri integraciji umetne inteligence v obstoječe sisteme ter prilagoditve obstoječih poslovnih procesov, kar je lahko časovno in finančno zahtevno.

Ugotovil sem, da večina podjetij, ki uporablja umetno inteligenco v kibernetški varnosti, opaža boljše rezultate v primerjavi s tradicionalnimi metodami, kar dokazuje njen potencial za izboljšanje zaščite. Kljub temu pa je še vedno veliko podjetij, ki bolj zaupajo tradicionalnim metodam ali pa se zanašajo na zunanje ponudnike storitev, kar je pri manjših podjetjih v večini edina možnost zaščite.

V prihodnje bi morala podjetja več pozornosti posvetiti usposabljanju zaposlenih za uporabo umetne inteligence ter vlaganju v napredne varnostne tehnologije. Ključno je tudi večje sodelovanje med podjetji in vladnimi organizacijami za razvoj ustreznih smernic ter zakonodaje, ki bi podprla varnostne prakse in zaščito pred napadi, ki vključujejo umetno inteligenco.

Za učinkovito obvladovanje kibernetških groženj je potrebno, da podjetja ne le vlagajo v tehnologijo, ampak tudi izobražujejo svoje zaposlene o digitalni varnosti ter spodbujajo sodelovanje med različnimi sektorji. Prav tako se mora večja pozornost nameniti odpravljanju pomanjkljivosti v zavedanju in izobraževanju, ki še vedno obstajajo v številnih organizacijah. S tem bomo zagotovili dolgoročno zaščito pred vse bolj naprednimi in kompleksnimi grožnjami v svetu kibernetške varnosti.

Naj zaključim z mislijo znanega ameriškega strokovnjaka za računalniško varnost, Bruce Schneierja, ki poudarja, da tehnologija sama po sebi ni dovolj za zagotavljanje kibernetške varnosti. Najpomembnejše je usposabljanje zaposlenih in upoštevanje kibernetške higijene.

"Če mislite, da lahko tehnologija reši vaše varnostne težave, potem ne razumete težav in ne razumete tehnologije." (Bruce Schneier)

## 6 VIRI IN LITERATURA

**Microsoft** [online]. What is Artificial Intelligence for Cybersecurity? [Povzeto 18. dec. 2024; 14:30]. Dostopno na spletnem naslovu: <https://www.microsoft.com/si-si/security/business/security-101/what-is-ai-for-cybersecurity>.

**SOLIX** [online]. Will Artificial Intelligence Take Over Cybersecurity? [Povzeto 18. dec. 2024; 14:40]. Dostopno na spletnem naslovu: <https://www.solix.com/si/blog/learning/will-ai-take-over-cyber-security/>.

**Ranktracker** [online]. The Role of Artificial Intelligence in the Cybersecurity Revolution. [Povzeto 18. dec. 2024; 14:50]. Dostopno na spletnem naslovu: <https://www.ranktracker.com/si/blog/artificial-intelligences-role-in-cyber-security-revolution/>.

**TechRadar** [online]. What is Artificial Intelligence? A Beginner's Guide. [Povzeto 18. dec. 2024; 14:50]. Dostopno na spletnem naslovu: <https://www.techradar.com/news/what-is-artificial-intelligence>.

**Forbes** [online]. The Impact of Artificial Intelligence on the Economy. [Povzeto 18. dec. 2024; 14:50]. Dostopno na spletnem naslovu: <https://www.forbes.com/sites/louiscolumbus/2019/11/04/10-charts-that-will-change-your-perspective-of-ai-in-security/>.

**Columbus, L.** (2019). 10 Charts That Will Change Your Perspective Of AI In Security. *Forbes*. [Povzeto 4. januar 2025]. Dostopno na spletnem naslovu: <https://www.forbes.com/sites/louiscolumbus/2019/11/04/10-charts-that-will-change-your-perspective-of-ai-in-security/>.

**Gov-is.si** [online]. Vpliv umetne inteligence na kibernetiko varnost. [Povzeto 18. dec. 2024; 14:30]. Dostopno na spletnem naslovu: <https://www.gov-is.si/objava/ID/1132/Vpliv-umetne-inteligence-na-kibernetiko-varnost>.

**Siceh.si** [online]. Uporaba in prihodnost umetne inteligence (AI) v kibernetiki varnosti. [Povzeto 18. dec. 2024; 14:30]. Dostopno na spletnem naslovu: <https://siceh.si/uporaba-in-prihodnost-umetne-inteligence-ai-v-kibernetiki-varnosti>.

**Stroka.si** [online]. Umetna inteligenca: grožnja in obramba v kibernetiki varnosti. [Povzeto 18. dec. 2024; 14:30]. Dostopno na spletnem naslovu: <https://www.stroka.si/Vsebina/Novice-in-obvestila/umetna-inteligenca-groznja-in-obramba-v-kibernetiki-varnosti>.

**Telekom.si** [online]. Kibernetiki napadi so vse bolj podprti z umetno inteligenco. Kako se lahko zaščitimo? [Povzeto 18. dec. 2024; 14:30]. Dostopno na spletnem naslovu: <https://www.telekom.si/tehnika/varnost-na-internetu/kibernetiki-napadi-so-vse-bolj-podprti-z-umetno-inteligenco-kako-se-lahko-zascitimo>.

**Microsoft** [online]. 10 essential insights from the Microsoft Digital Defense Report 2024 [Povzeto 7. mar. 2025; 16:20]. Dostopno na spletnem naslovu: <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/10-essential-insights-from-the-microsoft-digital-defense-report-2024#Daily%20malicious%20traffic%20volume-infographic>

**Microsoft** [online]. 10 essential insights from the Microsoft Digital Defense Report 2023 [Povzeto 7. mar. 2025; 16:30]. Dostopno na spletnem naslovu: <https://www.microsoft.com/en-us/security/security-insider/emerging-threats/microsoft-digital-defense-reports/10-essential-insights-from-the-microsoft-digital-defense-report-2023>

**Praček, A. in Vehovar, V.** (2024). Umetna inteligenca v Sloveniji 2024: uporaba in stališča. Center za družboslovno informatiko, Fakulteta za družbene vede, Univerza v Ljubljani. [Povzeto 9. marec 2025; 14:20]. Dostopno na spletnem naslovu: <https://www.uni-lj.si/assets/Kabinet/A-Novice/2024-12-19-raziskava-UI/Besedilo-raziskave-Umetna-inteligenca-v-Sloveniji-uporaba-in-stalisca.pdf>

## 7 PRILOGE

### Priloga 1

# Uporaba umetne inteligence za kibernetško varnost v Sloveniji

\* Nakazuje obvezno vprašanje

## 1. OSNOVNI PODATKI

1. 1.1 Ime podjetja/ustanove

---

2. 1.2. V katero panogo spada vaše podjetje? \*

*Označite samo en oval.*

- IT in telekomunikacije
- Bančništvo in finance
- Trgovina
- Proizvodnja
- Energetika
- Zdravstvo
- Transport
- Izobraževanje
- Javna uprava
- Zavarovalništvo
- Drugo:

3. 1.3. Koliko zaposlenih je v vašem podjetju? \*

*Označite samo en oval.*

- Manj kot 10
- 10–50
- 51–250
- 251–1000
- 1000–2000
- Več kot 2000

4. 1.4. Ali v vašem podjetju uporabljate umetno inteligenco? \*

*Označite samo en oval.*

- Da
- Ne, vendar to načrtujemo
- Ne

## 2. SPLOŠNA UPORABA UMETNE INTELIGENCE

5. 2.1. Na katerih področjih uporabljate umetno inteligenco v vašem podjetju?  
(Izberite vse, kar velja.)

*Izberite vse primerne odgovore.*

- Marketing in prodaja
- Optimizacija proizvodnih procesov
- Podpora strankam/uporabnikom
- Kibernetška varnost
- Drugo:  
\_\_\_\_\_

6. 2.2. Kako pogosto uporabljate umetno inteligenco pri vsakodnevem delu?

*Označite samo en oval.*

- Zelo pogosto
- Občasno
- Redko
- Nikoli

### 3. UPORABA UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI

7. 3.1. Ali v vašem podjetju uporabljate umetno inteligenco za zaščito pred kibernetškimi grožnjami? *Označite samo en oval.*

- Da, redno
- Da, občasno
- Ne, vendar to načrtujemo
- Ne

8. 3.2 Na katerih področjih kibernetške varnosti uporabljate umetno inteligenco? (Izberite vse, kar velja.)

*Izberite vse primerne odgovore.*

- Odkrivanje in preprečevanje napadov
- Upravljanje tveganj
- Analiza podatkov o grožnjah
- Varnost omrežja
- Drugo:

9. 3.3 Katere prednosti opažate pri uporabi umetne inteligenca na področju kibernetške varnosti? (Izberite največ tri.)

*Izberite vse primerne odgovore.*

- Hitrejše odkrivanje groženj
- Zmanjšanje stroškov varnosti
- Večja natančnost pri prepoznavanju napadov
- Avtomatizacija obrambnih sistemov
- Drugo:

10. 3.4. Katere so glavne ovire za širšo uporabo umetne inteligenca na področju kibernetške varnosti v vašem podjetju?

Izberite vse primerne odgovore.

- Visoki stroški implementacije
  - Pomanjkanje usposobljenih strokovnjakov
  - Pomanjkanje zaupanja v AI rešitve
  - Regulativne ovire
  - Drugo:
- 

11. 3.5 Kakšen vpliv ima uporaba umetne inteligence na vaše stroške na področju kibernetške varnosti?

Označite samo en oval.

- Stroški so se zmanjšali
- Stroški so ostali približno enaki
- Stroški so se povečali
- Ne vem

12. 3.6. Na lestvici od 1 do 10 ocenite, kako pomembna je uporaba umetne inteligence za izboljšanje kibernetške varnosti v vašem podjetju? (1 = sploh ni pomembna, 10 = ključnega pomena) Označite samo en oval.

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

13. 3.7. Kako ocenjujete učinkovitost umetne inteligence pri zaznavanju kibernetških groženj v primerjavi s tradicionalnimi metodami? (1 = manj učinkovita, 10 = veliko bolj učinkovita) Označite samo en oval.

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

14. 3.8. Katero področje kibernetške varnosti bi si po vašem mnenju lahko najbolj izboljšalo z uporabo umetne inteligence?

---

---

---

---

---

#### 4. PRIHODNOST UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI

15. 4.1. Ali menite, da bo umetna inteligenca v prihodnosti ključni element kibernetške varnosti?

*Označite samo en oval.*

- Zelo verjetno
- Verjetno
- Malo verjetno
- Sploh ne

16. 4.2. Ali v vašem podjetju opazate porast napadov na vaše strežnike, ki vključujejo uporabo umetne inteligence?

*Označite samo en oval.*

- Da, pogosto
- Da, vendar redko
- Ne
- Ne vem

17. 4.3. Kako se vaše podjetje pripravlja na obrambo pred napadi, ki vključujejo umetno inteligenco?

*Označite samo en oval.*

- Vlagamo v AI rešitve za obrambo
- Izvajamo redno usposabljanje zaposlenih
- Sodelujemo z zunanjimi ponudniki rešitev
- Nimamo posebnih priprav
- Drugo:

18. 4.4. Na lestvici od 1 do 10 ocenite, kako pripravljeno je vaše podjetje na obrambo pred kibernetškimi napadi, ki vključujejo uporabo umetne inteligence. (1 = sploh ni pripravljeno, 10 = popolnoma pripravljeno) *Označite samo en oval.*

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

19. 4.5. Kakšno vlogo pričakujete, da bo umetna inteligenca igrala pri zagotavljanju kibernetške varnosti v naslednjih petih letih?

---

---

---

---

---

## 5. DODATNA VPRAŠANJA

20. 5.1. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: **Stroški implementacije** *Označite samo en oval.*

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

1 2 3 4 5 6 7 8 9 10

21. 5.2. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: **Razpoložljivost strokovnjakov** *Označite samo en oval.*

1 2 3 4 5 6 7 8 9 10

---

---

22. 5.3. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: **Zaupanje v tehnologijo** *Označite samo en oval.*

1 2 3 4 5 6 7 8 9 10

---

---

23. 5.4. Na lestvici od 1 do 10 ocenite naslednji dejavnik, ki vpliva na uvedbo umetne inteligence v vašem podjetju: **Podpora vodstva** *Označite samo en oval.*

1 2 3 4 5 6 7 8 9 10

---

---

24. 5.5. Ali želite prejeti povzetek rezultatov raziskave? (vnesite svoj e-poštni naslov)

---