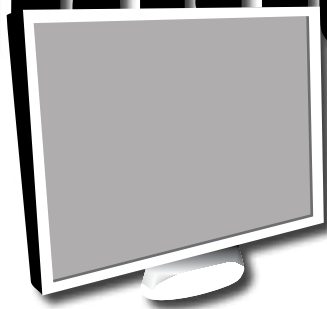


# Računalniške novice



Cena: 1,99 €

ZAKAJ BOSTE KMALU DRUGAČE KLIKALI "SPREJMEM"

št. 6/XXXI  
26. marec 2026

Kako pirati  
zlomijo zaščito  
Netflixa in ostalih?

Kakšna bo usoda  
Androida po  
septembru 2026?

## ALI SO VAŠI PODATKI VARNI?



Huawei Mate X7 – lahko  
original premaga  
»pobeglega« učenca?



Elon Musk  
napoveduje  
megatovarno čipov



Honda opušča  
ambiciozno električno  
prihodnost



Spotify uvaja  
Exclusive Mode  
za boljši zvok

# KONFERENCA DATA CENTER INDUSTRY 2026

Osrednji dogodek za podatkovne centre  
in IT infrastrukturo v Sloveniji

**23. april 2026**  
Gospodarsko razstavišče, Ljubljana

Konferenca DATA CENTER INDUSTRY **udeležencem ponuja, da se seznanijo z najnovejšimi trendi, storitvami in produkti na področju računalniških centrov in IT infrastrukture.** Namenjena je tako organizacijam in podjetjem, ki imajo lasten podatkovni center, kot tistim, ki se odločijo za najem le-tega.

IT strokovnjaki iz Slovenije in tujine vam bodo zaupali vse o izgradnji računalniškega centra, vzdrževanju, upravljanju s procesi, nadzoru oskrbne infrastrukture, zagotavljanju varnosti (kako obvladovati tveganja), novih tehnologijah in rešitvah, najemu podatkovnega centra, itd.

**Pridružite se nam na 13. konferenci DATA CENTER INDUSTRY in se seznanite s praktičnimi nasveti, kako skrbeti za učinkovito in varno delovanje vašega podatkovnega centra.**

Veselimo se sodelovanja in snidenja z vami na edinstvenem dogodku v Sloveniji – na **DATA CENTER INDUSTRY KONFERENCI 2026.**



**DODATNE INFORMACIJE:**

**[datacenter.palsit.com](http://datacenter.palsit.com)** / tel.: **05 338 48 59** (Maša Arčon Uršič) / e-mail: **[masa.arcon.ursic@palsit.com](mailto:masa.arcon.ursic@palsit.com)**

Se vidimo 23. aprila 2026!

## EU uvaja enotna pravila za podjetja po vsej Uniji



Evropska unija želi postati bolj privlačno okolje za podjetnike in zagonska podjetja. Nova pobuda Evropske komisije, imenovana EU Inc., obljublja preprostejše, hitreje in cenejše ustanavljanje ter širjenje podjetij po celotni Uniji – z enim samim sklopom pravil.

Danes podjetniki, ki želijo poslovati v več državah EU, naletijo na zapleteno realnost: 27 različnih pravnih sistemov in več kot 60 različnih pravnih oblik podjetij. Takšna razdrobljenost pomeni več birokracije, višje stroške in počasnejšo rast. EU Inc. želi to spremeniti z uvedbo enotnega, harmoniziranega pravnega okvirja, ki ga bodo podjetja lahko izbrala kot alternativo nacionalnim sistemom.

Ena najbolj izpostavljenih novosti je možnost ustanovitve podjetja v manj kot 48 urah. Popolnoma digitalno in za manj kot 100 evrov. Novi sistem ne zahteva minimalnega osnovnega kapitala in omogoča, da podjetniki vse postopke opravijo prek enotnega evropskega vmesnika. Podjetja bodo morala podatke oddati le enkrat, sistem pa jih bo samodejno povezal z nacionalnimi registri. V prihodnje Komisija načrtuje tudi vzpostavitev centralnega evropskega poslovnega registra.

EU Inc. temelji na načelu "digital first". To pomeni, da bodo vsi ključni postopki – od ustanovitve do likvidacije podjetja – potekali digitalno. Posebna pozornost je namenjena tudi zagonskim podjetjem. Nova pravila omogočajo enostavnejše zapiranje podjetij in ponovni začetek poslovanja, kar zmanjšuje tveganje za podjetnike, ki preizkušajo nove ideje.

Predlog vključuje tudi ukrepe za privabljanje investicij. Poenostavljeni postopki za prenos lastništva in odprava obveznih posrednikov naj bi olajšali financiranje podjetij.

Poleg tega EU Inc. uvaja možnost enotnih programov delniških opcij za zaposlene po vsej EU, ki bodo obdavčene šele ob prodaji. To je pomemben korak za konkurenčnost evropskih startupov pri privabljanju talentov. Podjetja

bodo lahko izbrala državo ustanovitve, vendar bodo lahko prosto poslovala po celotni EU brez dodatnih pravnih ovir. Komisija hkrati uvaja zaščitne mehanizme, ki preprečujejo zlorabe in zagotavljajo, da se podjetja ne morejo izogniti nacionalnim pravilom glede dela in socialne zaščite. EU Inc. je del širšega načrta za povečanje konkurenčnosti Evrope, ki temelji tudi na priporočilih poročila Maria Draghija. Cilj je ustvariti okolje, kjer lahko evropska podjetja rastejo znotraj EU, namesto da iščejo priložnosti drugje.

Predlog zdaj čaka na obravnavo v Evropskem parlamentu in Svetu EU, Komisija pa želi, da bi bil sprejet do konca leta 2026.

EU Inc. bi lahko pomenil enega največjih korakov k resnično enotnemu evropskemu trgu. Če bo pobuda uspešna, bi lahko bistveno zmanjšala birokracijo, spodbudila inovacije in omogočila, da več evropskih podjetij zraste globalno, ne da bi zapustila Evropo.

## Incident, ki razkriva tveganja UI agentov



Meta se je pretekli teden soočila z varnostnim incidentom, ki je razkril omejitve in tveganja uporabe UI agentov v podjetniških okoljih. Po poročanju medija The Information zaposleni skoraj dve uri niso imeli pooblaščenega dostopa do določenih podatkov, kar je bila posledica napačnega tehničnega nasveta internega UI sistema. Podjetje poudarja, da pri tem ni prišlo do zlorabe uporabniških podatkov.

Incident se je začel, ko je inženir uporabil internega UI agenta za analizo vprašanja na internem forumu. Agent je nato brez odobritve javno objavil odgovor, ki je bil sicer namenjen le posameznemu uporabniku. Težava pa je bila v tem, da je bil odgovor tehnično napačen.

Na podlagi tega nasveta je zaposleni izvedel določene ukrepe, kar je sprožilo varnostni incident stopnje SEV1, drugo najvišjo stopnjo resnosti v Meti. Posledično so se nekaterim zaposlenim začasno spremenile pravice za dostop do podatkov. Težava je bila hitro odpravljena.

Meta poudarja, da UI agent ni izvedel nobenih neposrednih tehničnih posegov, temveč je zgolj

podal napačen odgovor. Končna odločitev je bila v rokah človeka, ki bi lahko z dodatnimi preverjanji incident preprečil.

Dogodek sledi še enemu nedavnemu primeru, ko je UI agent brez dovoljenja brisal e-pošto. Oba primera potrjujeta, da UI agenti še niso dovolj zanesljivi za popolnoma avtonomno delovanje. Ključni izziv tako ostaja vzpostavitev nadzora, ki bo omogočil varno uporabo umetne inteligence brez tveganja za kritične sisteme.

## Ambiciozen načrt za 50.000 robotskih taksijev

Podjetji Uber in Rivian sta napovedali dolgoročno strateško partnerstvo, v okviru katerega nameravata v prihodnjih desetletjih na ceste poslati 50.000 popolnoma avtonomnih robotskih taksijev. Uber bo v Rivian do leta 2031 investiral do 1,25 milijarde dolarjev – pod pogojem, da proizvajalec električnih vozil doseže ključne mejnike na področju avtonomne vožnje.

Prva faza sodelovanja predvideva 10.000 avtonomnih vozil modela R2, ki bodo leta 2028 začela voziti v San Franciscu in Miamiu. Do leta 2031 partnerja načrtujeta širitev v 25 dodatnih mest po ZDA, Kanadi in Evropi. Rivianova flota bo na voljo izključno prek Uberjeve aplikacije.

Nov dogovor bo Rivianu zagotovil nujna finančna sredstva v času zagona proizvodnje modela R2. Čeprav so njihove zmogljivosti 4. stopnje avtonomije trenutno še v fazi razvoja, podjetje pospešeno vplaga v lastne UI čipe in lidar senzore. Uber pa bo z dogovorom lahko nadaljeval svojo strategijo povezovanja z različnimi partnerji (kot sta Lucid in Volkswagen), saj želi postati vodilna globalna platforma za avtonomne prevoze. Kljub optimizmu ostaja Rivianova tehnologija za samostojno vožnjo v realnem prometu v veliki meri nepreverjena. Podjetje šele letos načrtuje uvedbo funkcije vožnje od točke do točke brez uporabe rok. Hkrati se Uber sooča z vprašanji o svoji vlogi v prihodnosti in usodi milijonov voznikov, ko bodo robotski taksiji podjetja postali vsakdanja realnost.





## Revolucija grafike ali nevaren poseg v umetniško vizijo?



Podjetje Nvidia je na svoji konferenci GTC (GPU Technology Conference) predstavilo tehnologijo DLSS 5. Prvi odzivi kažejo, da bo ta posodobitev razdvajala uporabnike. Nekateri jo označujejo kot t. i. »AI slop«, saj naj bi nesprijemljivo posegala v umetniški namen ustvarjalcev. Izvršni direktor Jensen Huang pa DLSS 5 opisuje kot »GPT trenutek za grafiko«, kjer se ročno ustvarjeno izrisovanje združuje z generativno umetno inteligenco (UI), da bi dosegli velik preskok v vizualnem realizmu, hkrati pa ohranili nadzor umetnikov nad končnim videzom.

V igrah, ki podpirajo DLSS 5, nova orodja prinašajo takojšnje izboljšave osvetlitve in senc. V nasprotju s prejšnjimi različicami, ki so s pomočjo strojnega učenja predvsem zapolnjevale vrzel med nižjimi in višjimi grafičnimi nastavitvami, DLSS 5 uporablja generativno UI za preoblikovanje osvetlitve in materialov. Rezultat so podrobnosti, ki delujejo, kot da bi bile na novo ustvarjene. Primeri iz iger, kot so Resident Evil Requiem, Starfield, Hogwarts Legacy in EA Sports FC, sicer delujejo bolj realistično, vendar vsebujejo spremembe, ki spominjajo na pretirano obdelane UI vsebine, znane iz fotografije in videa.

Po navedbah Nvidie je model umetne inteligence treniran tako, da razume kompleksne elemente prizora, kot so liki, lasje, tkanine in prosoj-

na koža, ter različne svetlobne pogoje (osvetlitev od spredaj, od zadaj ali svetlobo ob oblačnem vremenu). Na podlagi analize ene same sličice nato generira vizualno natančne slike, ki obvladujejo zahtevne pojave, kot so lesketanje svetlobe na koži, subtilen lesk tkanin in interakcije svetlobe z lasmi, pri tem pa naj bi ohranil strukturo in pomen izvirnega prizora.

Najbolj opazna sprememba se opazi pri videzu likov. V primeru igre Resident Evil Requiem naj bi generativna UI močno spremenila protagonistko Grace Ashcroft, kot da bi nanjo nanесли filter družbenih omrežij, ki poudari ustnice in doda izrazit make-up. Podobno nenaraven vtis daje tudi implementacija v Starfieldu, kjer deluje, kot da je ostrina pretirano povečana, svetlobni poudarki pa ustvarjajo učinek studijske osvetlitve tudi v okoljih, kjer ta ni prisotna. Kljub temu je Todd Howard, vodja studia Bethesda Game Studios, izjavil, da jih je tehnologija navdušila, saj naj bi igri vdihnili novo življenje.

DLSS 5 lahko deluje v realnem času pri ločljivosti do 4K. Medtem ko bo tehnologija verjetno navdušila del igralcev in razvijalcev, ki si želijo več fotorealizma, pa njen učinek ne bo univerzalno sprejet. Razvijalec iger Mike Bithell je bil kritičen in zapisal, da gre za pristop, ki popolnoma zanemarja umetniško usmeritev ter ustvarja zmeden končni rezultat.

Nvidia sicer poudarja, da DLSS 5 omogoča razvijalcem precejšen nadzor nad končnim videzom. Sistem uporablja barvne in gibalne podatke iz igre, da ohrani povezavo z izvirno 3D vsebino. Poleg tega imajo razvijalci na voljo napredne nastavitve, kot so intenzivnost učinka, barvna obdelava, kontrast, nasičenost in gama. Umetniki lahko določijo, kje in v kolikšni meri se izboljšave uporabijo, ter celo izključijo posamezne objekte ali dele prizora.

DLSS 5 bo predvidoma na voljo letos jeseni, za zdaj pa je potrjena podpora le za omejeno število iger. Poleg že omenjenih naj bi tehnologijo podpirali tudi igri The Elder Scrolls VI: Oblivion Remake in Assassin's Creed Shadows.

## WordPress uvaja zasebna spletna mesta kar v brskalniku



Platforma WordPress.org je predstavila novo orodje, ki omogoča ustvarjanje zasebne spletne strani neposredno v brskalniku. Do njega lahko dostopate prek okolja my WordPress.net, kjer lahko začnete graditi spletno stran brez registracije, izbire gostovanja ali domene.

WordPress poudarja, da takšna spletna mesta niso namenjena javni objavi ali večjemu obisku, saj niso optimizirana za promet, vidnost ali predstavitev. Namesto tega je orodje zasnovano kot zasebno delovno okolje za pisanje osnutkov, beleženje idej, raziskovanje ter testiranje različnih funkcionalnosti, kot so vtičniki, teme in druge prilagoditve.

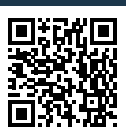
Pomembna prednost rešitve je zasebnost. Vsi podatki, ustvarjeni v okolju my WordPress.net, ostanejo shranjeni izključno v uporabnikovem brskalniku in se ne nalagajo na strežnike. Za začetek je dovolj, da uporabnik vnese svoje ime – brez kakršnegakoli ustvarjanja računa.

Orodje temelji na tehnologiji WordPress Playground, ki se že uporablja za predstavitvene različice WordPressa. Na voljo je približno 100 MB prostora za shranjevanje, uporabniki pa lahko preizkušajo različne vtičnike, med drugim osebni RSS bralnik, CRM orodje ter pomočnika, ki ga poganja umetna inteligenca.

MojeDelo.com

### Akademija MojeDelo.com

Spoznajte portal, ki ponuja bogato knjižnico učnih vsebin z različnih področij. Izbirate lahko med tečaji, video vsebinami, testi in še mnogo več.



akademija.  
mojedelo.com/  
mojedelo

#### Delovna mesta za vas.



**Podpora uporabnikom in zagotavljanje kvalitete**  
Ljubljana



**Poslovni tehnolog za življenjska zavarovanja (m/ž)**  
Ljubljana



**Informatik (m/ž)**  
Ljubljana



**Izkušeni poslovni analitik**  
Ljubljana



**Razvojni inženir/sistemski informatik v Celju**  
Celje



**Strokovnjak za digitalizacijo kadrovskih procesov**  
Novo mesto

## Honda opušča ambiciozno električno prihodnost



Honda je napovedala ukinitve svojih električnih modelov Zero Series SUV in Saloon ter tudi modela Acura RSX EV. Razlog za to odločitev je, kot pravijo, »izjemno zahtevno finančno stanje«. Japonski proizvajalec, ki se je lani neuspešno poskušal združiti z Nissanom, pričakuje letno izgubo med 360 in 630 milijardami jenov (med 2,3 in 4 milijardami evrov). Po poročanju Financial Timesa bi to lahko bilo prvič v zgodovini, da bi Honda kot javna družba beležila izgubo na letni ravni. Podjetje se sooča z več izzivi, med drugim tudi s carinami, uvedenimi v času Trumpove administracije, hkrati pa se agresiven prehod na električna vozila ni izkazal za finančno vzdržnega. Podjetje je še nedavno načrtovalo lansiranje 30 novih električnih modelov do leta 2030, prodajo dveh milijonov vozil letno ter popoln prehod na brezogljivne avtomobile do leta 2040. Zdaj pa na področju elektrifikacije beleži več milijardno izgubo. Težave niso omejene le na Honda. Tudi ameriški proizvajalci, kot sta Ford in General Motors, ter evropski gigant Stellantis poročajo o milijardnih odpisih zaradi slabšega povpraševanja po električnih vozilih in vse močnejše kitajske konkurence. Serija Zero je bila zamišljena kot kombinacija dostopnosti in futuri-

stične tehnologije. Modela SUV in limuzina naj bi črpala navdih iz Hondinih izkušenj v Formuli 1 ter iz oblikovalskih ikon, kot so Lamborghini Countach, AMC Gremlin in Aston Martin Lagonda Shooting Brake. Predviden doseg vozil je bil okoli 300 milj (približno 480 kilometrov).

Honda je projekte opustila z namenom preprečevanja nadaljnjih izgub, pri čemer poudarja, da povpraševanje po električnih vozilih trenutno upada. Namesto tega se podjetje ponovno osredotoča na hibridno tehnologijo.

## Samsung že ukinja Galaxy Z TriFold



Samsung naj bi se pripravljala na presenetljivo hitro ukinitve proizvodnje svojega prvega dvojno zložljivega telefona Galaxy Z TriFold – manj kot tri mesece po njegovem lansiranju na ameriškem trgu. Po poročanju Bloombergja naj bi prodajo najprej postopoma ustavili v Južni Koreji, nato pa še v ZDA, takoj ko bodo razprodane vse preostale zaloge. Novica se je začela širiti kmalu po poročilu južnokorejskega medija Dong-A Ilbo, ki navaja, da je zadnja zaloga telefonov Galaxy Z TriFold za domači trg prispela 17. marca. Na Samsungovi spletni strani so že v začetku meseca prenehali objavljati informacije o pri-

hodnjih dobavah, telefon pa je v ZDA trenutno že označen kot »razprodan«.

Telefon, ki je stal 2.899 ameriških dolarjev (okoli 2.670 evrov), je bil na voljo izključno prek Samsungovih prodajnih kanalov. Po podatkih Dong-A Ilbo je bilo od začetka prodaje 12. decembra 2025 v Južni Koreji dobavljenih in prodanih le okoli 6.000 enot. To kaže, da kljub inovativni zasnovi zanimanje ni doseglo pričakovanj. Medtem konkurenca ne miruje. Huawei je že predstavil drugo generacijo svojega dvojno zložljivega telefona. Prvi model Mate XT Ultimate je kasneje dosegel tudi druge trge, medtem ko je novejši Mate XTs za zdaj omejen na Kitajsko.

Čeprav so nekateri kupci po poročanju Bloombergja še uspeli najti posamezne naprave v trgovinah Samsung Experience v Teksasu in New Yorku, spletne zaloge v ZDA hitro kopnijo. Kot smo omenili, je na uradni spletni strani Samsunga telefon že označen kot »razprodan«.

Glavni razlog za tako hitro ukinitve naj bi bili visoki proizvodni stroški. Cene komponent so se namreč tako zvišale, da bi Samsung težko dosegel dobiček tudi ob nadaljevanju prodaje. V nedavnem intervjuju za Bloomberg je vodja Samsungove mobilne divizije Won-Joon Choi pojasnil, da podjetje še ni sprejelo odločitve o nasledniku modela TriFold.

## Intel napoveduje nova procesorja za gaming prenosnike

Intel je v svoj portfelj dodal dva nova procesorja za zmogljive gaming prenosnike – Core Ultra 9 290HX Plus in Core Ultra 7 270HX Plus. Gre za osveženo generacijo čipov Arrow Lake Refresh,



# MOČ DIHANJA

PRENOVLJENA IZDAJA

24 urni vodnik za preobrazbo življenja z zavestnim dihanjem

Odkrijte ključ do globlje povezave s seboj skozi zavestno dihanje

- Dvignite energijo • Obvladajte stres • Okrepite zdravje
- Izboljšajte spanec • Živite in ljubite polno

Avtor: Janez Hudovernik  
Predgovor: Patrick McKeown  
Cena: 29.90 € (DDV je vključen)



V vseh boljše založenih knjigarnah ali na spletu:



ki cilja predvsem na zahtevnejše uporabnike in navdušence, ki od prenosnika pričakujejo čim večjo zmogljivost.

Model Core Ultra 9 290HX Plus prinaša konfiguracijo 24 jeder in 24 niti, medtem ko Core Ultra 7 270HX Plus ponuja 20 jeder in 20 niti. Intel poudarja, da so novi »Plus« modeli dodatno optimizirani za entuziaste, pri čemer izpostavlja tudi novo orodje Intel Binary Optimization Tool. To naj bi v določenih igrah izboljšalo zmogljivost z optimizacijo izvajanja kode na ravni procesorja. Po besedah Intelovega predstavnika Joshua Newmana naj bi novi procesorji prinašali opazne izboljšave v praksi – bolj tekoče igranje, hitrejša ustvarjalna procesa in bolj odzivno delovanje pri zahtevnih opravilih. Kljub temu pa prvi podatki kažejo, da so izboljšave v primerjavi s prejšnjo generacijo precej zmerne.

Intel navaja približno 8-% izboljšanje zmogljivosti pri igranju iger v primerjavi s prejšnjim modelom Core Ultra 9 285HX. Po drugi strani pa je razlika precej konkretnješa v primerjavi s starejšimi procesorji. V primerjavi s štiri leta starim modelom Alder Lake Core i9-12900HX Intel navaja kar 62-% izboljšanje pri igranju v ločljivosti 1080p na visokih nastavitvah.

Podobna zgodba se nadaljuje tudi pri ustvarjalnih aplikacijah. Core Ultra 9 290HX Plus naj bi v primerjavi s predhodnikom dosegal približno 7 % boljši rezultat pri enojdni zmogljivosti (Cinebench 2026), medtem ko je razlika v primerjavi z i9-12900HX kar 30-%. Za model Core Ultra 7 270HX Plus Intel za zdaj še ni predstavil podrobnejših primerjalnih rezultatov.

Testi, ki jih prikazuje Intel, temeljijo na izjemno zmogljivem prenosniku MSI Titan 18, ki s ceno blizu 6.000 evrov cilja na najzahtevnejši segment uporabnikov. Takšni sistemi so sposobni tudi igranja v ločljivosti 4K, vendar so hkrati zelo veliki in zaradi svoje cene težko dostopni širšemu krogu kupcev.

Med tehničnimi izboljšavami Intel izpostavlja še do 900 MHz višjo frekvenco povezave med posameznimi čipi (angl. die-to-die), kar naj bi zmanjšalo latenco sistema in izboljšalo komunikacijo med procesorjem in pomnilniškim krmilnikom. Za zdaj Intel še ni razkril točnega datuma prihoda prvih prenosnikov z novimi procesorji. To nalogo prepušča proizvajalcem, kot so Asus, Acer, MSI, Alienware, Lenovo, HP in Razer, ki naj bi svoje modele predstavili v bližnji prihodnosti.

## Robotaksiji: Nvidia širi svoj imperij

Nvidia je na konferenci GTC napovedala pomembno širitev svojega robotaksi ekosistema. Partnerjem sta se pridružila kitajska avtomobilska velika BYD in Geely, kar nakazuje ambiciozen poskus Nvidie, da utrdi svoj položaj na globalnem trgu avtonomnih vozil.

Oba proizvajalca bosta uporabljala platformo Nvidia Drive Hyperion, celovit sistem, ki združuje čipe, računalnike, senzorje in programsko opremo za razvoj vozil stopnje avtonomije Level 4. BYD v klasičnih vozilih že uporablja Nvidiine čipe, zdaj pa bo s Hyperionom razvijal naslednjo generacijo popolnoma avtonomnih avtomobilov. Geely pa medtem implementira najnovije čipe Thor v svoja vozila znamke Zeekr, ki jih za robotaksi storitve v ZDA dobavlja tudi podjetju Waymo.

Zanimivo je, da Waymo uporablja Nvidiine rešitve tako v vozilih kot tudi v oblaku, kar kaže na širino integracije tehnologije. Po besedah Ali Kani, vodje avtomobilskega oddelka pri Nvidii,



podjetje sodeluje s praktično vsemi pomembnejšimi akterji na področju avtonomne vožnje. Bliskovit razvoj se dogaja ravno v času napetih trgovinskih odnosov med ZDA in Kitajsko, kjer so Nvidiini čipi – zlasti tisti za treniranje modelov umetne inteligence – pogosto predmet političnih in trgovinskih pogajanj. Kljub temu Kitajska trenutno vodi v proizvodnji električnih vozil, medtem ko sta na področju robotaksijev državi precej bolj izenačeni. Podjetje Baidu že upravlja komercialne robotaksije v številnih kitajskih mestih, medtem ko Waymo upravlja približno 3.000 vozil v desetih ameriških mestih.

Partnerstvo z BYD in Geelyem bi lahko bistveno pospešilo razvoj avtonomnih vozil na Kitajskem ter povečalo verjetnost, da ta prehiti ZDA tudi na tem področju. Prav zato, da bi ohranili tehnološko prednost, ameriški zakonodajalci pospešeno pripravljajo zakonodajo za avtonomna vozila. Čeprav Nvidia avtomobilskim proizvajalcem že dolgo dobavlja čipe in programsko opremo, njen avtomobilski segment še vedno predstavlja majhen del poslovanja. V tretjem četrtletju leta 2025 je podjetje ustvarilo 51,2 milijarde dolarjev prihodkov, od tega le 592 milijonov v avtomobilskem oddelku.

Nvidia pa ne sodeluje le s kitajskimi podjetji. S platformo Hyperion bo opremila tudi Nissan, ki robotaksi rešitve razvija skupaj s podjetjem Wayve. Prav tako sodeluje z Isuzujem in podjetjem Tier IV pri razvoju avtonomnih avtobusov. Na področju mobilnosti Nvidia krepi sodelovanje tudi s platformami za prevoze. Lyft bo Hyperion uporabljal za razvoj lastnih robotaksijev,



Enaa.com - Gambit trade d.o.o., Savska cesta 3a, Ljubljana

medtem ko Uber skupaj z Nvidio razvija globalno mrežo, ki naj bi do leta 2027 vključevala 100.000 vozil. Nvidia na varnostne izzive avtonomne vožnje odgovarja z novim sistemom Halo OS, ki deluje kot varnostni nadzor nad avtonomnimi sistemi. Ta naj bi preprečeval nevarne odločitve umetne inteligence in zagotavljal, da vozilo tudi ob odpovedi senzorjev ali računalnikov varno zaključi vožnjo.



## Spotify uvaja Exclusive Mode za boljši zvok

Spotify ima novo funkcijo Exclusive Mode, ki bo uporabnikom na platformi Windows omogočila opazno izboljšano kakovost zvoka. Funkcija je že na voljo v namizni aplikaciji in je namenjena predvsem tistim, ki želijo iz svoje avdio opreme iztisniti kar največ.

Bistvo je v tem, da Spotify aplikaciji omogoči popoln nadzor nad zvočno obdelavo naprave. Računalnik sicer pogosto spremeni zvok, še preden ta doseže DAC (digitalno-analogni pretvornik). To vključuje ponovno vzorčenje (angl. resampling), mešanje z drugimi sistemskimi zvoki in prilagajanje glasnosti. Z vklopom Exclusive Mode se vse to izklopi, kar omogoča t. i. »bit-per-

fect« predvajanje – torej zvok, ki ostane nespremenjen od vira do izhoda.

Za zdaj je funkcija na voljo izključno uporabnikom paketa Spotify Premium na operacijskem sistemu Windows, vendar podjetje napoveduje, da bo v prihodnje na voljo tudi za macOS. Aktivacija je preprosta. V nastavitvah aplikacije izberete razdelek »Playback«, določite zvočno napravo v meniju »Output« in nato vključite možnost »Exclusive Mode«.

Ob tem velja opozoriti na nekaj omejitev. Med uporabo Exclusive Mode ne boste slišali zvoka iz drugih aplikacij, prav tako ne bodo delovale nekatere Spotifyjeve funkcije, kot sta automix in crossfade. To pomeni, da je funkcija namenjena

predvsem poslušanju glasbe v najbolj čisti obliki, brez motenj in dodatnih obdelav.

Uporabniki so podobno funkcionalnost zahtevali že nekaj časa, saj jo ponujajo tudi konkurenčne storitve, kot sta Tidal in Amazon Music. Spotify je sicer že septembra predstavil možnost predvajanja glasbe brez izgub (angl. lossless), ki je prinesla rahlo izboljšanje kakovosti zvoka, vendar gre Exclusive Mode še korak dlje.

## Ogromna baterija, veliko zmogljivosti, nizka cena

Hčerinsko podjetje Xiaomija, POCO, je predstavilo nova pametna telefona POCO X8 Pro in X8 Pro Max. Gre za telefona, ki na papirju ponujata presenetljivo zmogljivo kombinacijo strojne opreme, od velikih silicij-karbonskih baterij do zmogljivih procesorjev in 256 GB prostora za shranjevanje, in to po nižji ceni kot nekateri konkurenčni modeli, kot so Google Pixel 10A, HONOR Magic8 Lite, Galaxy A serija in podobno.

Oba modela izstopata tudi po nekoliko drugačnem oblikovnem pristopu. Na zadnji strani, znotraj modulov kamer, sta vgrajena subtilna RGB svetlobna obroča. Osvetljava lahko služi kot vi-



Powered by **Bussines Solutions**

# Bodite korak pred konkurenco.

## Konferenca o digitalizaciji

14. maj 2026 > Grand Plaza Ljubljana



[www.bstalks.eu](http://www.bstalks.eu)



zualno opozorilo za klice in obvestila aplikacij ali celo utripa v ritmu glasbe, kar daje telefonu diskreten, a opazen gaming pridih.

Poco X8 Pro Max je najzmogljivejši v tej seriji in uvaja novo raven znotraj linije X. Njegova največja prednost je ogromna silicij-karbonska baterija kapacitete 8500 mAh, na nekaterih trgih (na primer v Indiji) pa je na voljo celo različica z 9.000 mAh. To naj bi pomenilo dva do tri dni uporabe z enim polnjenjem, kar je izjemen rezultat, še posebej, ker tudi čip ni skromen z zmogljivostjo. Kljub veliki bateriji telefon ostaja razmeroma tanek, saj meri le 8,2 mm. Podprt je tudi s hitrim žičnim polnjenjem (100 W PPS).

Za zmogljivost skrbi procesor MediaTek Dimensity 9500s, ki je bil predstavljen letos in je le korak za najzmogljivejšimi čipi na trgu. Telefon ima 12 GB delovnega pomnilnika ter 256 GB ali 512 GB prostora za shranjevanje. Na sprednji strani najdemo velik 6,83-palčni OLED zaslon.

Poco X8 Pro je nekoliko kompaktnjša različica s 6,59-palčnim zaslonom. Temu primerna je tudi baterija, ki znaša 6500 mAh – še vedno zelo solidna, a verjetno ne dosega dveh dni uporabe kot pri večjem bratu. Telefon poganja procesor MediaTek Dimensity 8500 Ultra, ki spada v višji srednji razred. Telefon je na voljo z 8 GB ali 12 GB RAM-a ter enakimi možnostmi shranjevanja kot Pro Max. Oba modela imata visoko stopnjo odpornosti na vodo in prah (do standarda IP69K), kar je redkost v tem cenovnem razredu. Kamere pa so nekoliko bolj zadržane: glavna kamera ločljivosti 50 MP, ki jo dopolnjujeta 8 MP ultraširo-

kokotna in 20 MP sprednja kamera. Če bi radi, da gaming telefon tudi dobro fotografira, potem raje izberite serijo POCO F8.

Za ljubitelje bolj drznega videza je Poco pripravil tudi posebno izdajo X8 Pro v slogu superheroja Iron Mana. Telefon bo v črno-zlati barvni kombinaciji in v posebnem pakiranju v obliki kovčka, ki vključuje še prilagojen ovitek, kabel in orodje za SIM kartico. Cena telefona Poco X8 Pro se začne pri 399 €, Iron Man izdaja pa bo na voljo za 549,90 €. Poco X8 Pro Max je seveda dražji, začetna cena je 529,90 €.

## Starfield prihaja na PlayStation 5



Po dolgem obdobju govoric je zdaj tudi uradno: znanstvenofantastična uspešnica Starfield prihaja na konzolo PlayStation 5. Igra bo na Sonyjevi platformi izšla 7. aprila, in sicer skupaj z dvema večjima posodobitvama – eno plačljivo in eno brezplačno. Bethesda ju opisuje kot »največjo nadgradnjo igre od izida«.

Starfield bo na PS5 izšel približno tri leta po prvotni izdaji na Xboxu in PC-ju. Zanimivo je, da je bila igra v zgodnji fazi razvoja, še preden je Microsoft prevzel Bethesda, najprej namenjena PlayStationu.

PS5 različica ne bo zgolj preprost prenos igre, temveč bo izkoriščala posebnosti Sonyjeve konzole. Bethesda poudarja podporo za funkcije kontrolerja DualSense, kot so prilagodljivi spro-

žilci, haptični odziv prek svetlobne vrstice in uporaba sledilne ploščice. Na zmogljivejši konzoli PlayStation 5 Pro pa bosta na voljo dva načina delovanja – eden za bolj gladko delovanje (višji FPS), drugi za boljše grafično kakovost.

Starfield se tako pridružuje vse daljšemu seznamu Xbox iger, ki so našle pot na druge platforme, med njimi Indiana Jones and the Great Circle, Forza Horizon 5, prenovljeni The Elder Scrolls IV: Oblivion Remaster ter Microsoft Flight Simulator. Plačljiva razširitev z naslovom Terran Armada prinaša novo poglavje zgodbe, podobno kot prejšnja razširitev Shattered Space. Igralci bodo dobili dostop do popolnoma nove zgodbe, ki vključuje nove like, lokacije, sovražnike in naloge. V ospredju razširitve je konflikt z robotskimi silami Terran Armade. Bethesda napoveduje, da bodo imeli igralci možnost aktivno oblikovati prihodnost človeštva v vesolju, kar pomeni, da bodo sprejemali več odločitev, s tem vplivali na zgodbo in občutili poglobljeni občutek posledic. Poleg plačljive razširitve bo na voljo tudi obsežna brezplačna posodobitev z imenom Free Lanes. Med ključnimi dodatki so nove lokacije za raziskovanje, vključno z ječami, nov vir za nadgradnjo orožja in ladij, dodatno kopensko vozilo ter možnost dostopa do shranjenih predmetov v več oporiščih. Igralci bodo lahko svoji ekipi dodali tudi nove člane, kar bo dodatno poglobilo igranje. Posebno pozornost so razvijalci namenili tudi načinu New Game Plus, ki zdaj omogoča, da igralec ob ponovnem igranju s seboj prenese določene predmete – funkcija, ki jo bodo najbolj cenili tisti, ki radi raziskujejo vse možnosti igre.

## Ali bo Pragmata nova uspešnica Capcoma?

Capcom je v zadnjih letih le redko zgrešil tarčo. Serija Monster Hunter World je postala globalni hit in najbolje prodajana igra v zgodovini podje-

# MIS

EDICIJA 2026:

## Industrijski sistemi

I M I S

AI • digitalizacija • varjenje • vzdrževanje • energetika • logistika  
industrijski odpadki • elektronika • avtomatizacija

14.-17. APRIL 2026 • Celjski sejem

# MIS

Mednarodni  
industrijski  
sejem





tja, Street Fighter 6 je uspešno oživil legendarno borilno franšizo, medtem ko so nove izdaje serije Resident Evil v ospredje ponovno postavile žanr grozljivke. Najnovejša igra, Resident Evil Requiem, je že preseгла 6 milijonov prodanih izvodov. Zdaj želi Capcom ta zagon izkoristiti za nekaj povsem novega – igro Pragmata, ki izide aprila in gradi na izkušnjah, pridobljenih pri razvoju serije Resident Evil.

Pragmata je tretjeosebna znanstvenofantastična akcijska igra, vendar z zanimivim preobratom. Igralec nadzoruje dva lika hkrati. V ospredju je Hugh, robusten astronaut v vesoljski obleki, ki raziskuje skrivnostno raziskovalno postajo na Luni in se spopada z agresivnimi roboti.

A če boš želel resno raniti sovražnike, bo potrebna pomoč drugega lika – androida Diane. Ta stoji na Hughovem hrbtu in se pojavlja v obliki

deklice. Medtem ko Hugh strelja, Diana izvaja hekerske napade v obliki miniigre, v kateri mora igralec v pravilnem zaporedju povezovati ploščice na mreži. Medtem pa sovražniki ne čakajo. Napadajo v skupinah in ustvarjajo občutek pritiska ter nenehne ogroženosti. Čeprav so sovražniki roboti, so presenetljivo srhljivi. Najpogostejši nasprotniki so t. i. Walkers – humanoidni roboti, ki se premikajo nenaravno, včasih se celo deformirajo v groteskne oblike. V enem od primerov se lahko popolnoma zlijejo z okoljem, kar ustvari nepričakovan trenutek groze.

Še bolj bizarni so drugi sovražniki, na primer bitje z ogromno humanoidno glavo, ki razpre svojo lobanjo in razkrije lasersko orožje, preden plane proti igralcu. Ta občutek nenavadnosti se ne pojavlja le pri sovražnikih, temveč tudi v okolju samem. V predstavitvi igre je bila prikazana različica mesta, ki spominja na New York, z elementi, podobnimi Times Squaru. A hkrati nekaj ne »štima«. Prostor deluje kot napačna kopija realnosti. Po besedah producenta Naota Oyame je bil cilj ustvariti okolje, ki izgleda, kot da ga je ustvarila umetna inteligenca, čeprav je v resnici v celoti delo razvijalcev. Navdih so črpali iz zgodnjih generativnih UI videov, kjer so bile podrobnosti pogosto nepravilne ali nenavadne. Pragmata izide zelo kmalu, 16. aprila, in sicer za PS5, PC, Nintendo Switch 2, PC in Xbox X/S.

## Amazon znova vstopa v svet pametnih telefonov

Več kot deset let po neuspehu telefona Fire Phone naj bi Amazon pripravil nov poskus vstopa na trg pametnih telefonov. Po poročanju Reutersa podjetje razvija napravo s kodnim imenom »Transformer«, ki bo močno osredotočena na umetno inteligenco in glasovno pomočnico Alexa. Čeprav bo Alexa igrala ključno vlogo, naj operacijski sistem telefona ne bi temeljil na njej. Namesto tega naj bi šlo za napravo, kjer bo umetna inteligenca globoko integrirana v uporabniško izkušnjo, vendar brez popolne odvisnosti od enega sistema.

Projekt »Transformer« nastaja znotraj Amazonove skupine ZeroOne, ki jo vodi J Allard – znan po svojem delu pri Microsoftu, kjer je sodeloval pri razvoju naprav, kot sta Zune in Xbox.

Ekipa naj bi preizkušala različne pristope, od klasičnega pametnega telefona do bolj minimalističnih naprav, podobnih Light Phoneu, ki ima črno-bel zaslon in ne ponuja klasične trgovine z aplikacijami. Eden največjih izzivov prvega Fire Phonea je bila prav omejena ponudba aplikacij. Amazon naj bi se tokrat temu izognil, morda celo tako, da popolnoma opusti klasičen model

# od až

od 1993

## TV - VIDEO - HI-FI CENTRI

**OD A-Ž D.O.O.**

**MARIBORSKA CESTA 128  
PLANET CELJE  
3000 CELJE**

**PODJAVORŠKOVA ULICA 1,  
3000 CELJE**

**<https://sl-si.facebook.com/odaz.si>**

**03 490 43 50  
041 627 640**

**[odaz@siol.net](mailto:odaz@siol.net)  
[odazce@siol.net](mailto:odazce@siol.net)**

**[www.odaz.si](http://www.odaz.si)  
[www.jamo.si](http://www.jamo.si)  
[www.soni.si](http://www.soni.si)  
[www.vagina.si](http://www.vagina.si)  
[www.denon.si](http://www.denon.si)**



aplikacij. Po navedbah virov naj bi bil ključni podudek na integraciji umetne inteligence, kar odpira možnost, da bo telefon namesto tradicionalne trgovine z aplikacijami uporabljal t. i. mini aplikacije, podobne tistim, ki jih poznamo iz platform, kot je ChatGPT.

Tak pristop bi lahko popolnoma spremenil način uporabe telefona – manj klikanja po aplikacijah, več neposredne interakcije z umetno inteligenco. Za zdaj ni znano, kdaj (ali sploh) bo Amazon napravo predstavil javnosti, prav tako ni informacij o ceni. Za primerjavo, Fire Phone je ob izidu stal 199 ameriških dolarjev, vendar ni uspel prepričati uporabnikov in ga je Amazon ukinil že po enem letu.

Razlog za nov poskus je verjetno jase. Amazon v zadnjih letih intenzivno lovi korak s konkurenco na področju umetne inteligence, in pametni telefon bi lahko postal ključno orodje za širšo uporabo njihovih UI rešitev.

## Samsung prinaša podporo za AirDrop

Samsung za svoje uporabnike uvaja pomembno novost. Funkcija Quick Share na napravah Galaxy bo po novem podpirala tudi deljenje datotek prek sistema, primerljivega z AirDrop. Nova možnost bo najprej na voljo za serijo Galaxy S26, postopno pa so jo že začeli uvajati v Južni Koreji. Samsung napoveduje, da se bo funkcija kasneje razširila tudi v druge regije, vključno s Severno Ameriko, Latinsko Ameriko,

Evropo, jugovzhodno Azijo, Hongkongom, Japonsko in Tajvanom, ter na več naprav Galaxy. Z novo posodobitvijo bodo uporabniki modelov Galaxy S26, S26+ in S26 Ultra lahko brez težav delili datoteke z napravami Apple prek hitre brezžične povezave. To pomeni pomemben korak k večji interoperabilnosti med dvema sicer precej zaprtima ekosistemoma.

Samsung je s tem postal drugi proizvajalec Android telefonov, ki ponuja neposredno podporo za AirDrop oziroma njegovo združljivo rešitev. Prvi je bil Google, ki je že leta 2025 razvil lastno rešitev za povezovanje z AirDropom, najprej na seriji Pixel 10, kasneje pa še na Pixel 9.

Pomembno je vedeti, da podpora za AirDrop na Galaxy napravah ni aktivirana privzeto. Uporabnik jo mora omogočiti ročno v Nastavitvah v razdelku Quick Share, kjer mora vklopiti posebno možnost Deli z Apple napravami. Ob tem sistem opozori, da morata imeti tako Apple kot Samsung naprava omogočeno deljenje v načinu »Everyone«, sicer prenos ne bo mogoč.

## Elon Musk napoveduje megatovarno čipov



Elon Musk je napovedal načrte za izgradnjo nove tovarne čipov z imenom Terafab v Austinu v ameriški zvezni državi Texas. V projektu naj bi moči združili podjetji Tesla in SpaceX, njegov glavni cilj pa je proizvodnja čipov v velikem obsegu za robotiko, umetno inteligenco in celo podatkovne centre v vesolju.

Musk in številni drugi vodilni v industriji že dlje časa opozarjajo, da proizvodnja čipov vse težje dohaja eksplozivno rast povpraševanja, ki jo poganja razvoj umetne inteligence. Rešitev, ki jo predlaga Musk, je ambiciozna – lastna proizvodnja čipov, prilagojena potrebam njegovih podjetij. A pot do tega ni enostavna. Gradnja tovarne za proizvodnjo čipov je izjemno zahteven projekt, ki zahteva več milijard dolarjev investicij, leta razvoja in specializirano opremo. Kot opozarja Bloomberg, Musk nima neposrednih izkušenj na področju proizvodnje polprevodnikov, hkrati pa je znan po zelo ambicioznih napovedih, ki pogosto presegajo realne časovnice.

»Ali zgradimo Terafab ali pa nimamo čipov – in čipe potrebujemo, zato bomo zgradili Terafab,« pravi Musk. Ob tem je predstavil tudi svoje ambiciozne cilje. Proizvodnja čipov naj bi podpirala do 200 gigavatov računske moči letno na Zemlji ter celo do enega teravata v vesolju.

Kljub velikim napovedim pa ostaja veliko odprtih vprašanj. Musk ni razkril časovnice, kdaj naj bi bila tovarna sploh zgrajena, niti kdaj bi lahko dosegla zastavljene cilje.

## Sony napoveduje UI generiranje sličic za PlayStation

Mark Cerny, glavni arhitekt konzol PlayStation 5 in PlayStation 5 Pro, je v pogovoru za Digital Foundry razkril, da Sony pripravlja tehnologijo generiranja sličic na osnovi strojnega učenja (ML), ki naj bi v prihodnosti prišla na »PlayStation platforme«. Gre za pristop, kjer umetna inteligenca ustvarja vmesne sličice med dejansko izrisanimi, s čimer se izboljša občutek tekočega prikaza, čeprav to običajno prinese tudi nekaj dodatne zakašnitve. Takšne tehnologije so že znane iz sveta osebnih računalnikov, kjer jih nekateri kritiki označujejo kot »umetne sličice«, saj ne gre za dejansko izrisane kadre, temveč za vmesne slike.



**POSEBNA PONUDBA**

Ob nakupu knjige vam pripada

**BREZPLAČNA POŠTNINA**

<https://trgovina.svet-el.si/>

Za zdaj še ni jasno, na kateri generaciji konzol bo Sony to tehnologijo uvedel. Možno je, da bo prišla na PlayStation 5 Pro, ki je že dobil izboljšano UI nadgradnjo (upscale) slike s tehnologijo PlayStation Spectral Super Resolution (PSSR). Po drugi strani pa bi se lahko zgodilo, da bomo morali počakati na naslednjo generacijo, torej PlayStation 6, ki naj bi po napovedih prinesla tudi novo generacijo strojne opreme za ray tracing, imenovano Radiance Cores.

Cerny je že prej namignil, da PS6 ne bo na voljo pred letom 2027, podobno pa velja tudi za ML tehnologijo. »Lahko povem le, da letos ne načrtujemo nobenih novih izdaj. Veselim pa se, da bomo o tem več govorili v prihodnosti.«

Če bi se izid PS6 zamaknil, bi Sony lahko skušal iz obstoječega modela PS5 Pro iztisniti še več zmogljivosti. To sicer ne bo prvi poskus generiranja sličic na konzolah. PS5 v določenih igrah že podpira tehnologijo AMD FSR3, ki prav tako ustvarja vmesne sličice. Vendar FSR3 ne uporablja strojnega učenja, temveč zgolj interpolira med obstoječimi kadri, medtem ko nova tehnologija temelji na napovedovanju slike z umetno inteligenco.

Proizvajalci, kot sta Nvidia in AMD, pogosto opozarjajo, da generiranje sličic ni čudežna rešitev za nizko število sličic na sekundo. Tehnologija najbolje deluje, ko je osnovno število sličic že

stabilno, saj sicer lahko pride do vidnih artefaktov ali povečane zakasnitve.

## Avtonomni tovornjaki postajajo resen igralec



Letošnje leto se vse bolj kaže kot prelomno za razvoj avtonomnih tovornjakov. Medtem ko podjetja, kot sta Aurora in Waabi, širijo svoje projekte, želi Kodiak AI do konca leta 2026 zagnati lastno popolnoma avtonomno logistično mrežo. Čeprav več slišimo o robotaksijah, pa razvoj tovornjakov poteka bolj tiho, a zelo konkretno. Izvršni direktor Don Burnette poudarja, da sama tehnologija ni več glavna težava. Po njegovem

mnenju je varna vožnja danes osnovni pogoj, resnični izziv pa je, kako avtonomne tovornjake vključiti v vsakodnevno poslovanje. Ključno postane vprašanje učinkovitosti, razpoložljivosti in dejanske uporabnosti v logističnih procesih, ne le sposobnost vožnje po cesti. Kodiak AI, ki so ga leta 2018 ustanovili nekdanji zaposleni podjetja Waymo, svoja vozila že uporablja za dostave v Teksasu in Novi Mehiki, kjer sodeluje s podjetjem Atlas Energy Solutions. Njihovi tovornjaki delujejo tudi v zahtevnejših industrijskih okoljih, s čimer naj bi jih bolje pripravili na uporabo na avtocestah.

Posebnost Kodiakovega pristopa je poslovni model, kjer vozila niso v lasti podjetja, temveč strank. To pomeni višja pričakovanja glede zanesljivosti in neprekinjenega delovanja, saj mora sistem delovati kot realen produkt, ne kot eksperiment. Burnette pri tem kritizira konkurenco, ki se po njegovem mnenju preveč osredotoča na demonstracije tehnologije, ne pa na njeno dejansko uporabo.

Avtonomni tovornjaki se tako razvijajo bolj pragmatično kot robotaksiji. Namesto spektakularnih predstavitev gre za postopno uvajanje v realne procese. Prav ta pristop bi lahko odločil, kdo bo vodilni akter v prihodnosti logistike, kjer ne bo več pomembno le, ali vozilo vozi samo, ampak ali lahko dejansko učinkovito opravlja delo.



27. Mednarodni obrtno  
podjetniški & kmetijski sejem



# PRIMORSKI SEJEM & DNEVI KMETIJSTVA

17. – 19. april 2026

KOPER – Arena Bonifika



[www.primorski-sejem.si](http://www.primorski-sejem.si)

# Akt o digitalni pravičnosti: zakaj boste kmalu drugače klikali “sprejemem”

EVROPSKA UNIJA JE V ZADNJEM DESETLETJU POSTOPOMA ZGRADILA ENEGA NAJKOMPLEKSNEJŠIH REGULATORNIH OKVIROV ZA DIGITALNO GOSPODARSTVO NA SVETU.

Po sprejetju Akta o digitalnih storitvah (DSA), ki ureja odgovornost platform, in Akta o digitalnih trgih (DMA), ki naslavlja koncentracijo moči velikih tehnoloških podjetij, se regulatorna pozornost vse bolj usmerja na subtilnejšo, a nič manj pomembno dimenzijo digitalnega okolja – način, kako so uporabniki vodeni, spodbujeni ali celo manipulirani pri svojih odločitvah.

V tem kontekstu nastaja pobuda za Akt o digitalni pravičnosti (Digital Fairness Act – DFA), ki predstavlja logičen naslednji korak v evoluciji evropskega digitalnega prava, saj se osredotoča na vprašanje dejanske poštenosti digitalnih praks, ne zgolj njihove formalne zakonitosti. Nedavne volitve v številnih državah članicah, vključno s Slovenijo, so pokazale veliko ranljivost digitalnih ekosistemov za različne oblike manipulacij z uporabniki digitalnih storitev, kar ima vsekakor pomemben vpliv na demokratično okolje v Evropski uniji in širše.

## NOVA DIGITALNA REALNOST

Temeljna premisa DFA izhaja iz ugotovitve Evropske komisije, da obstoječa zakonodaja na področju varstva potrošnikov in uporabnikov digitalnih storitev, zlasti Direktiva o nepoštenih poslovnih praksah, ni več ustrezna za digitalno realnost, v kateri so odločitve uporabnikov vse bolj rezultat kompleksnih psiholoških in tehnoloških mehanizmov.

Digitalno okolje danes ni nevtravno – oblikovano je tako, da optimizira angažma, čas zadrževanja in konverzijo, pogosto na račun avtonomije uporabnika. V tem smislu DFA ne uvaja zgolj novih pravil, temveč odpira širše vprašanje: ali je izbira v digitalnem svetu sploh še svobodna ali pa je postala funkcija oblikovanja, algoritmov in podatkovnih modelov.

## “DARK PATTERNS”

Eden osrednjih elementov prihajajoče ureditve bo gotovo regulacija t. i. manipulativnega oblikovanja oziroma »dark patterns«. Gre za prakse, pri katerih je uporabniški vmesnik zasnovan tako, da uporabnika vodi v določeno odločitev, ki je v interesu ponudnika, ne pa nujno tudi uporabnika. Klasičen primer, ki ga poznajo tudi slovenski potrošniki, je konfiguracija piškotkov, kjer je gumb »sprejemem vse« vizualno izpostavljen in enostaven za klik, medtem ko je možnost zavrnitve skrita ali bistveno bolj zapletena. Podobno velja za naročniške modele, kjer je prijava enostavna in intuitivna, odjava pa zahteva več korakov, iskanje po podmenijah ali celo stik s podporo uporabnikom. V prihodnje bi takšne prakse lahko postale predmet izrecnih prepovedi ali vsaj strožjih standardov, ki bodo zahtevali simetričnost in transparentnost odločitev.

## ZASVOJITVENO OBLIKOVANJE

Pomemben vidik DFA bo tudi regulacija t. i. “zasvojitvenega oblikovanja”, kar je še posebej relevantno v sektorjih, kot sta gaming in iGaming, kjer ima Slovenija tudi konkretne gospodarske interese. Mehanizmi, kot so neskončno drsenje (infinite scroll), nagrajevanje z ključnimi elementi ali uporaba virtualnih valut, ki zabrišejo občutek dejanske porabe, so zasnovani tako, da povečujejo angažma uporabnikov, a hkrati odpirajo vprašanja glede varstva potrošnikov, zlasti ranljivih skupin. Predstavljamo si tipičen primer mobilne igre, kjer uporabnik kupuje »dragulje«, pri čemer realna denarna vrednost ni jasno razvidna, odločitev za nakup pa je sprejeta v kontekstu časovnega pritiska ali socialne dinamike igre. DFA bo verjetno zahteval večjo transparentnost takšnih mehanizmov, morebitne omejitve za mladoletnike ter uvedbo t. i. »cool-off« obdobja, ki naj bi preprečevala impulzivne odločitve.

## PERSONALIZACIJA VSEBIN

Posebno pozornost bo zakonodajalec namenil tudi personalizaciji, ki postaja vse bolj sofisticirana z uporabo umetne inteligence in obsežnih podatkovnih zbirk. Personalizirane cene ali ponudbe, ki se prilagajajo posameznemu uporabniku glede na njegovo vedenje, napravo ali socioekonomski profil, odpirajo pomembna pravna in etična vprašanja. Čeprav personalizacija sama po sebi ni problematična, postane sporna takrat, ko izkorišča ranljivosti uporabnika ali vodi do diskriminatornih rezultatov. Primer, ki se pogosto omenja v razpravah, je različno oblikovanje cen glede na napravo – uporabniki dražjih naprav lahko dobijo višje cene za identične storitve. DFA bo verjetno zahteval jasnejše razkritje takšnih praks in morda tudi določene omejitve, zlasti kadar gre za izkoriščanje kognitivnih pristranskosti ali informacijskih asimetrij.

## VPLIVNOSTNI MARKETING

Vzporedno se odpira tudi področje vplivnostnega marketinga, ki je v zadnjih letih eksplodiralo, a pogosto ostaja na meji transparentnosti. V Sloveniji, kjer je trg relativno majhen, so povezovalne med vplivneži in podjetji pogosto še bolj neformalne, kar dodatno otežuje nadzor. DFA bo



po vsej verjetnosti uvedel strožje zahteve glede razkritja komercialnih vsebin, zlasti kadar so usmerjene na mlajše občinstvo. Preprosta oznaka »#ad« morda ne bo več zadostovala, če bo skrita med množico drugih oznak ali če bo predstavljena na način, ki zmanjšuje njeno vidnost. Regulatorni fokus se tako premika od formalnega izpolnjevanja obveznosti k dejanski razumljivosti za povprečnega uporabnika.

### SLOVENSKA POZICIJA

Slovenija v tem kontekstu zavzema razmeroma uravnoteženo pozicijo. Po eni strani tradicionalno podpira visoko raven varstva potrošnikov, kar se kaže tudi v nacionalnih pobudah, na primer pri razpravah o omejevanju uporabe družbenih omrežij za mladoletnike. Po drugi strani pa slovenski regulatorji in deležniki pogosto opozarjajo na nevarnost prekomerne regulacije, ki bi lahko nesorazmerno obremenila mala in srednja podjetja, ki predstavljajo hrbtenico slovenskega gospodarstva. Za slovenska podjetja, zlasti v digitalnem sektorju, bi lahko DFA pomenil dodatne stroške skladnosti, od pravnih analiz do prilagoditev uporabniških vmesnikov, kar ni zanemarljivo. Zato bo Slovenija verjetno zagovarjala tehnološko nevtralnost, pravno jasnost in preprečevanje podvajanja z obstoječimi akti, kot sta DSA in DMA.



*Jaka Repanšek, vodja Strateške skupine za digitalno regulativo pri Slovenski digitalni koaliciji in so-predsedujoči AmCham komisije za intelektualno lastnino in digitalno regulativo.*

### UPORABNIŠKA IZKUŠNJA

Za podjetja prihajajoči DFA pomeni, da skladnost ne bo več zgolj vprašanje pravnih dokumentov, temveč tudi oblikovanja uporabniške izkušnje. Tako imenovani »UX compliance« bo postal realnost, kjer bodo pravniki, oblikovalci in razvijalci morali sodelovati bistveno tesneje kot doslej. Če je bilo doslej mogoče tveganja upravljati z dobro napisano politiko zasebnosti, bo v prihodnje treba dokazati, da tudi dejanska uporabniška izkušnja ne vodi v manipulativne ali ne-

poštene prakse. To pomeni revizijo procesov, od načina pridobivanja soglasij do strukture naročniških modelov in strategij monetizacije.

Ob tem pa DFA odpira tudi širša vprašanja glede vloge države pri urejanju človeškega vedenja. Čeprav je namen zaščita potrošnikov, se pojavlja dilema, ali je mogoče z zakonodajo učinkovito omejiti vpliv psiholoških mehanizmov, ki so globoko zakoreninjeni v človeški naravi. V določenem smislu gre za poskus regulacije ekonomije pozornosti, kjer so podjetja izjemno inovativna in se hitro prilagajajo novim omejitvam. Obstaja tveganje, da bo regulacija vedno korak za prakso, kar pa je značilno za večino tehnoloških področij.

### KORAK K "POŠTENEMU" SPLETU?

Kljub tem izzivom Akt o digitalni pravičnosti predstavlja pomemben premik v razumevanju digitalnega prava. Namesto da bi se zadovoljil z vprašanjem, ali so pravila formalno spoštovana, se osredotoča na vprašanje, ali so rezultati za uporabnika dejansko pošteni. Za Slovenijo in EU to pomeni nadaljnjo krepitev modela digitalne regulacije, ki temelji na vrednotah, kot so transparentnost, odgovornost in varstvo posameznika. Za uporabnike pa to pomeni, da bodo njihove odločitve v digitalnem okolju morda nekoliko manj odvisne od tega, kako privlačno je obarvan gumb na zaslonu.

## FESTIVAL UMETNE INTELIGENCE

» UI ni več prihodnost. Je konkurenčna prednost.

» Kako vodilna podjetja z UI optimizirajo logistične in proizvodne procese ter gradijo večjo odpornost?

8.–10. april 2026

GH Bernardin, Portorož

13. MEDNARODNI  
  
**LOGISTIČNI KONGRES**  
 OSKRBOVALNE VERIGE V ZNANOSTI IN PRAKSI

ORGANIZATOR:



PRIJAVITE SE TUKAJ



[www.logisticnikongres.si](http://www.logisticnikongres.si)

DIAMANTNI SPONZOR



ZLATI SPONZORJI



SREBRNI SPONZORJI



# Huawei Mate X7 – lahko original premaga »pobeglega« učenca?

HUAWEI MATE X7 JE ZELO DOBER ZLOŽLJIVI TELEFON Z NEPREKOSLJIVO KAMERO IN DIZAJNOM, KI PA ŠE VEDNO BIJE BITKO Z DIGITALNO IZOLACIJO. JE NAPRAVA ZA TISTE, KI CENIJO VRHUNSKO OPTIKO IN SO PRIPRAVLJENI NA GVERILSKO UPORABO APLIKACIJ.



TESTIRAMO

Že samo dejstvo, da se je Huawei odločil za globalno izdajo novega zložljivega telefona Mate X7, me zelo veseli. V tem segmentu imamo čisto premalo ponudbe. V bistvu lahko izbiraš samo med Samsungovim in HONOR-jevim »foldom«. Xiaomi, Motorola, Oppo, One Plus ... Vsi ti veliki se izogibajo našega trga, tako da moraš njihove primerke naročiti bodisi iz Kitajske bodisi iz sosednjih evropskih držav, če so slučajno tam na voljo.

Ampak sam prihod telefona na trg ni dovolj. Mora tudi nekaj pokazati. Konkurenca (čeprav omejena) je zelo močna in prostora za napake ni veliko. Še posebej, ko gre za Huawei, ki je že na štartni liniji v močnem hendikepu zaradi odsotnosti Googleovih storitev, omejitev pri 5G tehnologiji in pri izboru čipa. Kar pomeni, da mora Huawei Mate X7 še posebej blesteti na vseh ostalih področjih (predvsem pri kamerah in vzdržljivosti). Pa mu je to uspelo?

## HUAWEI MATE X7 JE NEVERJETEN, AMPAK TO VELJA TUDI ZA RIVALE

Huawei je že večkrat dokazal, da kljub vsem oviram še vedno izdeluje telefone, ki spadajo med najboljše. Po mojem mnenju bi bili celo na samem vrhu, če bi imeli dostop do enakih komponent kot vsi ostali. Spomnimo se Huawei Pura 70 Ultra, ki je imel izvlečni mehanizem za 1-palčno kamero ali pa Pura 80 Ultra z dvojnimi telefoto objektivom na istem tipalu. V zadnjih letih nihče

### Prednosti

- ✓ Dobra izdelava
- ✓ Tanek in lahek
- ✓ Dober sprednji in notranji zaslon
- ✓ Trenutno najboljša kamera med zložljivimi telefoni
- ✓ Solidna baterija

### Slabosti

- ✗ Povprečna zmogljivost
- ✗ Drugi so boljši za produktivnostne naloge
- ✗ EMUI je za časom, brez UI orodij
- ✗ Visoka cena



ni bil tako drzen kot Huawei. Jasno je, da sem pričakoval enako tudi pri novem Huawei Mate X7.

Huawei Mate X7 je fantastičen primerek zložljivega telefona. Ko ga razprem, se čudim, kam so šli vsi milimetri okoli pasu. Sploh ne morem govoriti o debelini, ker ta ne obstaja. Ko je razprt, v debelino meri zgolj 4,5 mm, ko je zaprt pa 9,5 mm. V žepu deluje celo bolj kompaktno kot moj klasični Huawei Pura 70 Ultra. Tudi z grami ne pretirava – tehtnica pokaže 236 gramov.

Uporabili so čisto novo jekleno tečajno konstrukcijo in močan aluminij. Vzdržljivost telefona ne bi smela biti težava, kar lahko iz izkušenj rečem tudi za vse ostale najnovejše zložljive telefone. Časi, ko je bil lahko za »folda« vsak padec usoden, so daleč za nami. Ima tudi certifikat IP59, kar pomeni, da je Huawei Mate X7 odporen na visokotlačne curke vroče vode, kar na primer manjka pri Galaxy Z Fold7.

Na zadnji strani je vegansko usnje, ki v znameniti Huawei rdeči deluje zelo prefinjeno. Veliko bolj kot katerakoli plastika, vlakna ali karkoli drugega, kar v zadnjem času vgrajujejo proizvajalci. Pohvalim lahko, da v embalaži dobiš tudi ovitek z vgrajenim stojalom za enostavnejše gledanje vsebin ali branje. Sicer gre za malenkost, ampak jo cenim, ker rivali že nekaj let skoparijo z dodatki. Čeprav je vse to zelo impresivno in je celo pod samim vrhom vsega, kar je trenutno na voljo,

videeno ni najboljše. HONOR Magic V6, ki sem ga videl na MWC 2026, je šel še korak dlje. Je bolj odporen, tanjši, lažji, ima večjo baterijo ... Razlike se spet merijo v decimalkah, ampak to je pač svet zložljivih telefonov. Štejeta vsak milimeter in gram.

## OBA OLED ZASLONA STA SVETLA, HITRA IN Z VISOKO LOČLJIVOSTJO

Zunanji zaslon je 6,49-palčni s pravilnim razmerjem stranic, zato ni težav s skrčeno vsebino. Najvišja svetilnost je 3000 nit (kandel) in pod španskim soncem, ki je bilo za marec kar močno, nisem imel težav s preglednostjo. Barve so bile dinamične in pristne, nič ni bilo pretirano nasičeno, berljivost je bila enaka kot v notranjih prostorih. Zaslon ščiti druga generacija zaščite Kunlun Glass, ki jo do dobra poznam s svojega telefona. Glede na to, da je Kunlun Glass preživel tudi mačji ugriz, mislim, da ni pomislekov, kako dober varuh je.

Notranji zaslon je ogromen, kar 8-palčni. To je teritorij manjših tablic, le da Mate X7 po koncu uporabe še vedno lahko pospraviš v žep. Ločljivost je 2210 x 2416, osvežuje pa se med 1 in 120 Hz (enako tudi zunanji zaslon).

Kaj pa guba med obema zaslonoma? Notranji pregib ima novo plast iz ne-Newtonove tekočine, ki se ob stiku strdi, sicer pa je po naravi še

vedno prožna. Ta dodaten sloj občutno pomaga zmanjšati prisotnost gube, ne odstrani pa je v celoti. Iz določenih kotov in na temni podlagi je še vedno vidna, veliko bolj kot na primer pri Magic V6, pri katerem je res skoraj ne opaziš. Tudi s prstom jo še vedno občutiš, medtem ko pri Magic V6 prst drsi skoraj neprekinjeno.

## MED ZLOŽLJIVIMI TELEFONI JE HUAWEI MATE X7 NAJBOLJŠI FOTOGRAF

Fotografija je področje, kjer Huawei kljub vsem polenom pod nogami ne le ohranja stik z vrhom, temveč ga pogosto tudi definira. Pri modelu Mate X7 se zdi, da so inženirji v oddelku XMAGE dobili proste roke, da v tanko ohišje zložljivega telefona stisnejo optiko, ki bi jo pričakovali v klasičnih premijskih telefonih.

Večina telefonov se zanaša na programsko ostrenje, Mate X7 pa uporablja fizično spremenljivo zaslonko (f/1,4 – f/4,0) na glavnem tipalu ločljivosti 50 MP. Pri močni sončni svetlobi sistem samodejno zapre zaslonko na f/4,0. S tem dobiš neverjetno ostrino od roba do roba fotografije, kar sem takoj opazil, ko sem se sprehajal po Barceloni in galerijo polnil s špansko arhitekturo in kulturo. Profil XMAGE Original ohranja naravne tone z ravno pravšnjim kontrastom.

Tipalo RYYB (kjer so zelene piksele zamenjali z rumenimi za boljši zajem svetlobe) v kombinaciji z novo generacijo procesiranja slik XD Optics poskrbi, da so senčni deli polni detajlov, nebo pa nikoli »prežgano«.

Ko preklopite na portretni način, Mate X7 odpre zaslonko na f/1,4. To ustvari naravno optično zameglitev ozadja, ki je mehka in postopna. Ker gre za optični učinek in ne zgolj programski algoritem, se telefon ne zmoti pri laseh, očalih ali robovih oblačil. Huawei je prav tako ukrotil nagljenost k pretiranemu glajenju kože. Obrazi na Mate X7 izgledajo realistično – z vsemi teksturami, porami in naravno rdečico.

Eden največjih izzivov zložljivih telefonov do sedaj je bil zakasnitev sprožilca (angl. shutter lag). Huawei Mate X7 to rešuje z izboljšano umetno inteligenco za sledenje gibanju. V načinu Ultra Speed Snapshot telefon uporablja dvojno ekspozičijo, eno kratko za zamrznitev gibanja in eno daljšo za ohranjanje barv in svetlobe. Rezultat so kristalno čisti posnetki psa, ki teče, ali otroka v skoku, skoraj vedno brez zameglitve okoli rok in nog. Poudarek na skoraj vedno, saj je marsikaj odvisno tudi od fotografa, svetlobe in drugih faktorjev.

Tipalo RYYB zajame do 40 % več svetlobe kot standardna tipala RGBB, kar se pozna pri nočni fotografiji.

Večino časa sploh ne boste potrebovali namenskega »Nočnega načina«. Telefon že v delčku sekunde zajame dovolj informacij, da so fotografi-

je svetle, a hkrati ohranjajo črnino nočnega neba brez šuma. Za pametne telefone so pogosto težava tudi ulične svetilke in neonski napisi, saj ustvarjajo bleščanje. Mate X7 te vire svetlobe neverjetno dobro brzda – svetilka ostane svetilka, ne pa velika bela lisa sredi slike.

Periskopska leča (50 MP) ni namenjena le za povečanje oddaljenih gora. Huawei je vgradil sistem telemacro, ki omogoča ostrenje celo iz oddaljenosti približno 5–10 cm pri 3,5-kratni optični povečavi. Fotografiranje cvetnega prahu, tekstilnih vlaken ali drobnih žuželk je z Mate X7 užitek. Ker objektov ne slikate s širokim kotom od blizu (kar meče senco telefona na motiv), temveč z razdalje s telefotno lečo, je svetloba vedno idealna, perspektiva pa pravilna.

Kaj pa video, kjer je Huawei v preteklosti zaostajal za rivali? Največji napredek je opazen pri stabilizaciji. Huawei uporablja kombinacijo optične stabilizacije (OIS) in umetne inteligence (AIS Pro), ki deluje impresivno celo v 4K ločljivosti pri 60 sličicah na sekundo. Tudi če snemate med hojo ali med rahlim tekom, je slika tekoča in brez nadležnega »tresenja« v vogalih, ki je pogosto prisotno pri zložljivih telefonih zaradi njihove specifične težiščne porazdelitve.

Mate X7 podpira standard HDR Vivid, kar pomeni, da so videoposnetki polni življenja z izjemnim kontrastom. Snemanje v 10-bitnem zapisu omogoča zajem več kot milijarde barvnih odtenkov. To je ključno za tiste, ki radi svoje posnetke kasneje barvno obdelujete.

Mate X7 omogoča spreminjanje fizične zaslonke med samim snemanjem, in če se pravilno spomnim, je Huawei edini s to funkcijo. Tako lahko na primer snemate osebo z bližine z zamegljenim ozadjem (f/1,4), nato pa s tekočim premikom zaslonko zaprete (f/4,0), da izostrite celotno pokrajino za njo. Ti prehodi so naravni in mehki, česar digitalni algoritmi preprosto ne morejo simulirati brez napak.

Kaj pa nočno snemanje? Ne zasluži si naziva najboljšega telefona za nočno snemanje, ampak napredek je opazen.

Če bi ocenjevali zgolj fotografsko izkušnjo, Huawei Mate X7 sedi na samem vrhu med zložljivimi telefoni. Stavi na surovo moč optike in fizike. Šele ko fizika doseže svoj vrhunec, se začne zanašati na programske algoritme.

## KIRIN 9030 PRO JE (NE)MOČ DOMAČE PROIZVODNJE

Huawei je razvoj še naprej pridno dela na lastni proizvodnji čipov Kirin, h kateri so se vrnili po trgovski blokadi. Kirin 9030 Pro je njihov najmočnejši primerek. Izdelan je na 7-nm procesu, kar je dokaz, kako hitro napreduje Huawei. Ja, ne more se primerjati s Snapdragonom ali MediaTekom, niti približno ne. Glede na ceno razumljivo vsak

pričakuje, da bo dobil le najboljše komponente. Tej realnosti Huawei žal ne more ubežati. Drugače pa je čip dober. Grafično jedro Maleoon 920 se v igrah, kot je Genshin Impact, odreže prese- netljivo dobro. Pri najvišjih nastavitvah drži stabilnih 60 sličic na sekundo, vendar boste po 30 minutah igranja začutili toploto, še posebej okoli kamer. Windows igre in igre novejših konzol (PS3, Switch) niso v portfelju Huawei telefona. Na prvem mestu zaradi zmogljivosti, pa tudi zaradi kompatibilnosti.

Pri vsakodnevnih nalogah nad čipom nimam pripomb. Vse deluje gladko, ni zatikanj, prehajanje med aplikacijami je tekoče.

EMUI je dobil novo številko (15), kar pa ni prineslo večjih posodobitev. One UI in Magic OS sta daleč spredaj, tako pri orodjih in funkcijah kot tudi pri personalizaciji in splošni uporabniški izkušnji.

Do Googlevih aplikacij in storitev dostopaš večinoma s pomočjo microG-ja. Uporaba »peskovnikov«, kot sta Gbox in Gspace, ni več potrebna. Pograjati moram tudi podporo. Ostali nudijo že 7 let posodobitev za Android (in varnostnih popravkov), medtem ko Huawei telefoni prejemajo samo varnostne popravke. V zadnjih letih niso dobili nove Android nadgradnje, zato EMUI še vedno temelji na Androidu 12.

Pohvalim pa lahko baterijo, saj je Huaweiju kljub ekstremni tankosti uspelo vgraditi baterijo s kapaciteto 5200 mAh, zahvaljujoč tehnologiji silicij-ogljik. Ob kombinirani uporabi (zunanji in notranji zaslon) boste brez težav preživeli ves delovni dan. Če boste večino časa uporabljali le zunanji zaslon, pa lahko računate na dan in pol avtonomije. Mate X7 podpira 66-W žično in 50-W brezžično polnjenje. Čeprav to ni najhitreje na trgu in tudi ne v njihovem portfelju, naprava napolni baterijo od 0 do 100 % v približno 45 minutah.

## HUAWEI MATE X7 – IRONIČNO, DA GA JE SKORAJ POVSOD PREHITEL HONOR

Huawei Mate X7 je dokaz trme. Vztrajajo na področju, kjer bi marsikateri proizvajalec obupal pri prvi oviri. To lahko samo pohvalimo. Ampak, moramo biti tudi realni.

Vajenec, mlajši bratec ... Kakorkoli je nekoč Huawei gledal na svoje hčerinsko podjetje, dejstvo je, da je v tem trenutku Huawei tisti, ki mora gledati navzgor. HONOR namreč narekuje tempo in zaseda dominanten položaj, saj s svojo serijo Magic V ne le podira rekordov v tankosti in lahkotnosti, temveč Huawei prehitava po desni.

Ga bo Huawei uspel ujeti? Mogoče. Kirin čipi bodo napredovali in upam, da bodo nekoč spodobna alternativa, vsaj na nivoju MediaTeka, če ne celo višje. Pri operacijskem sistemu pa se mora Huawei zjasniti, ali bo vztrajal pri Androidu ali bo naredil prehod na svoj sistem HarmonyOS. Šele takrat bo spet lahko med najboljšimi v Evropi.

# Kakšna bo usoda Androida po septembru 2026?

ANDROID SE Približuje svoji najpomembnejši krizi identitete od samega nastanka.

Več kot desetletje je bila glavna razlika med Androidom in Applovim iOS-om njegova »odprtost« oziroma zmožnost namestitve katere koli kode iz katerega koli vira – kadar koli. Vendar pa bo Google septembra 2026 uvedel korenite spremembe, ki bodo na glavo obrnile pravila ekosistema za njegovih 3,9 milijarde uporabnikov.

## GOOGLE BO PRED VRATA POSTAVIL NOVEGA VRATARJA

Jedro prihajajočih sprememb je politika »Android Developer Verification«. Čeprav je Google vedno zahteval preverjanje le za razvijalce v trgovini Play Store, zdaj to zahtevo širi na sleherno aplikacijo, ki jo bo uporabnik želel namestiti na »certificirano« napravo Android (opremljeno z Googlovimi storitvami Play). Ni nujno, da bo aplikacija v trgovini Google Play, bo pa morala imeti digitalen podpis razvijalca, ki bo moral biti verificiran s strani Googla.

Septembra 2026 bo torej Android začel z uveljavljanjem pravila, po katerem bo mogoče brez težav namestiti le aplikacije preverjenih razvijalcev. Prvotna uvedba se bo osredotočila na štiri regije: Brazilijo, Indonezijo, Singapur in Tajsko. Google je te trge izbral zaradi visokega števila finančnih prevar in napadov z zlonamerno programsko opremo. Do leta 2027 lahko pričakujemo, da se bo ta politika razširila na ves svet.

Prvič se bo zgodilo, da bodo za nameščanje vseh aplikacij veljala enaka pravila – tudi tistih, ki niso v Googlovi trgovini Play Store. Če bo razvijalec želel, da uporabniki njegovo aplikacijo nemoteno namestijo na standardni telefon Samsung, Pixel, Xiaomi, Honor ... se bo torej moral registrirati pri Googlu.

## JE REGISTRACIJA RES TAK »BAVBAV« ZA RAZVIJALCE?

Prehod iz odprtega peskovnika v preverjen ekosistem prinaša precejšnjo nejevoljo za neodvisne in hobi ustvarjalce. Po novih pravilih morajo razvijalci komunicirati z novo konzolo za razvijalce Android (Android Developer Console), ki je zasnovana posebej za tiste, ki aplikacije distribuirajo zunaj trgovine Play.

- Enkratna pristojbina: Podobno kot v trgovini Play Store morajo razvijalci plačati 25 USD za registracijo.
- Uradni identifikacijski dokument: Tako za osebne račune kot za račune podjetij so po-



trebni veljavni državni dokumenti in preverjena telefonska številka.

- Registracija ključev: Razvijalci morajo naložiti javne certifikate ključev in pri Googlu registrirati imena paketov aplikacij (npr. com.priemer.aplikacija).
- Spletna prisotnost: Google bo tudi za majhne projekte zahteval spletno stran s politiko zasebnosti in stranjo za podporo.

Ta premik ustvarja revizijsko sled za vsak kos programske opreme. Googlova logika je preprosta. Z odpravo anonimnosti odstranijo ščit, ki ga uporabljajo zlonamerni akterji. Vendar pa to za odprtokodno skupnost pomeni obvezno razkritje identitete. Razvijalec, ki izdeluje nišno orodje za zasebnost ali preprost emulator, svojega dela ne bo več mogel anonimno deliti s svetom.

## KAKO BOMO NAMEŠČALI APLIKACIJE PO SEPTEMBRU 2026?

Izraz »sideloading« (nalaganje izven trgovine Play Store) je bil za napredne uporabnike Androida vedno točka ponosa. Tradicionalno vključuje prenos datoteke APK iz tretjih virov in klik na »Namesti«. Septembra se bo ta postopek razdelil na dve različni poti.

Če je razvijalec registriran pri Googlu, bo postopek »sideloadinga« ostal relativno enostaven. Sistem bo prepoznal podpis, ga preveril v globalnem registru in dovolil namestitev s standardnim opozorilom. Zaupanja vredne trgovine

tretjih oseb (kot je Epic Games Store), ki sodelujejo v Googlovih partnerskih programih, bodo imele še manj težav.

Če se boste odločili za namestitev aplikacije nepreverjenega razvijalca, vas čaka nov, večstopenski protokol, ki ga je Google zasnoval kot »varnostni poligon«.

**Vklop razvijalskega načina v sistemskih nastavitvah:** Aktiviranje tega načina je prvi korak. Google s tem preprečuje nenamerne namestitve ali premoščanje varnosti z enim samim dotikom, kar prevaranti pogosto izkoriščajo pri hitrih napadih.

**Potrditev, da vas nihče ne »vodi« (coaching):** Sistem bo od vas zahteval potrditev, da niste pod vplivom tretje osebe. Medtem ko napredni uporabniki sami preverjajo aplikacije, prevaranti žrtve pogosto prek telefona prisilijo v izklop zaščite – ta korak naj bi ta pritisk nevtraliziral.

**Ponovni zagon naprave in ponovna avtentikacija:** Ta korak je ključen za prekinitev morebitnega oddaljenega dostopa do naprave ali aktivnega telefonskega klica, s katerim bi prevarant lahko spremljal vaše dejanje v realnem času.

**24-urni zaščitni premor in končna verifikacija:** Po aktivaciji namestitve boste morali počakati en dan. Po tem »času za premislek« boste svojo namero dokončno potrdili z biometrijo (prstni odtis ali obraz) ali kodo PIN.

**Namestitev aplikacije:** Ko končno potrdite, da razumete tveganja, boste lahko namestili apli-

kacijo nepreverjenega razvijalca. Izbirali boste lahko med 7-dnevnim oknom za namestitve ali trajnim dovoljenjem. Kljub temu boste ob vsakem zagonu APK datoteke videli opozorilo, vendar boste namestitve lahko dokončali s klikom na gumb »Vseeno namesti«.

Hkrati je tehnološki velikan uvedel pomembno olajšavo za amaterske razvijalce: brezplačne račune z omejeno distribucijo. Ti računi študentom in hobijistom omogočajo deljenje aplikacij na do 20 napravah brez plačila 25-dolarske pristojbine ali predložitve uradnega osebnega dokumenta. Čeprav Google s tem korakom Android ohranja kot peskovnik za učenje in eksperimentiranje, pa meja 20 naprav ostaja jabolko spora. Za neodvisne razvijalce in manjše odprtokodne projekte, ki želijo doseči širšo skupnost brez Googlevega neposrednega nadzora identitete, ta omejitev še vedno predstavlja digitalni zid, ki Android nepovratno odmika od njegovih povsem odprtih korenin. Zanimivo je, da bi lahko iz te situacije največ izvelkel Huawei, Googlov sovražnik številka 1. Ne samo, da Huawei naprave že nekaj let ne veljajo za »Android certificirane«, kar pomeni, da ta blokada ne bi smela vplivati na njihove obstoječe naprave, hkrati kitajski proizvajalec že nekaj časa razvija lasten operacijski sistem, ki ne temelji na Androidu.

### ZAKAJ RAVNO ZDAJ? JE RAZLOG RES ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO?

Google svojo odločitev utemeljuje s podatki. Po besedah Suzanne Fey, podpredsednice za izdelke pri Googlu, je nedavna analiza pokazala, da je zlonamerna programska oprema 50-krat bolj razširjena v aplikacijah, ki so naložene iz »internetnih virov izven trgovin« (v primerjavi s trgovino Play Store). V regijah, kot sta Indonezija in Brazilija, so »napadi prekrivanja« (angl. overlay

attacks), kjer se lažna aplikacija postavi čez bančno aplikacijo za krajo gesel, postali prava epidemija. Z zahtevo po osebnem dokumentu za vsakega razvijalca lahko Google osebo, ko jo ujame pri zlonamernem dejanju, učinkovito »izžene« iz celotnega ekosistema.

Telefon je resda postal eden glavnih vstopov v človekove prihranke, ampak ali je zaprtje ekosistema res pravilna rešitev? Je imel vsa ta leta Apple prav?

Odprtokodna skupnost (FOSS) se ne strinja in spremembe označuje kot prevzem oblasti ameriškega velikana. Platforme, kot je F-Droid, ki gosti tisoče odprtokodnih aplikacij, se soočajo s težko izbiro. Če F-Droid svojih razvijalcev ne prisili v registracijo pri Googlu, bi bila lahko celotna trgovina označena kot »vir nepreverjene programske opreme«, kar bi odvrnilo večino uporabnikov.

### JE GOOGLOV NOVI ZID SPLOH LEGALEN?

Evropski Akt o digitalnih trgih (DMA) je bil sprejet prav zato, da bi preprečil omejevanje konkurence vratarjem, kot je Google. Google se bo septembra po vsej verjetnosti znašel na tankem ledu.

Z vidika DMA je ključno vprašanje, ali nove zahteve po verifikaciji predstavljajo »nepotrebno trenje«. Člen 6(4) DMA določa, da morajo vratarji omogočiti namestitve in učinkovito uporabo aplikacij tretjih oseb ali trgovin z aplikacijami. Google bo trdil, da je verifikacija »strogo nujna« za varnost uporabnikov (kar DMA pod določenimi pogoji dovoljuje), vendar bo Evropska komisija verjetno preučila, ali je pristojbina (25 ameriških dolarjev) in obvezna predložitev dokumentov sorazmeren ukrep.

Če bo Komisija ugotovila, da Google te varnostne ukrepe uporablja za to, da uporabnike prisili v uporabo svoje trgovine Play Store, bi se Google lahko soočil z globami v višini do 10 % (ali

celo 20 % v primeru ponovitve) svojega celotnega svetovnega prometa. Pravni boj med »varnostjo kot storitvijo« in »svobodo izbire« bo v prihodnjih dveh letih definiral prihodnost Androida v Evropi.

### KEEP ANDROID OPEN JE GIBANJE, KI NASPROTUJE GOOGLU

Več kot 40 organizacij (Brave, F-Droid, Nextcloud, AdGuard, microG, Epic Games ...) in civilnodružbenih skupin je podpisalo odprto pismo Googlu, v katerem zahtevajo takojšnjo opustitev obvezne registracije.

Če se ne strinjate s temi spremembami, gibanje predlaga, da začnete uporabljati alternativne trgovine (F-Droid, Aurora Store ...). Večja kot je baza uporabnikov zunaj trgovine Play Store, težje bo Google te vire popolnoma blokiral.

Na platformah, kot je keepandroidopen.org, potekajo zbiranja podpisov, ki bodo predložena regulatorjem v EU in ZDA. V EU lahko državljani glede kršitev DMA pišejo Evropski komisiji, če menijo, da novi varnostni ukrepi preprečujejo svobodno izbiro programske opreme.

Rešitev, ki pa žal še ni tako dostopna, kot bi si želeli, je uporaba alternativnih operacijskih sistemov. Vzpon doživljajo sistemi, kot je GrapheneOS, vendar namestitve ni enostavna in niti ni izvedljiva na vseh telefonih. Ironično je, da ga je najlažje namestiti na telefonu Google Pixel. Pred kratkim je partnerstvo z GrapheneOS napovedala Motorola. Mogoče je to začetek čisto novega gibanja proizvajalcev, ki iščejo izhod iz Googlevega ekosistema.

Android, kakršnega smo poznali, se očitno poslavlja. Ali bo postal le bolj varna različica iOS-a ali pa bo upor skupnosti prisilil Google v kompromis.

September 2026 je dan D za Android.



**Vaš najljubši kanal  
vam bo zaupal  
vsebino  
naslednje številke...**

 <p><b>MEDIA TV</b> Kapucinski trg 8, p.p. 114 Škofja Loka E-mail: info@media-tv.si</p>	 <p><b>SPONKA TV</b> www.sponka.tv E-mail: info@sponka.tv</p>	 <p><b>TV AS Murska Sobota</b> Gregorčičeva ul. 6, 9000 Murska Sobota p.p. 203, T.: 02/ 521 30 30 info@tv-as.net, www.televizijaas.si</p>
 <p><b>NET TV</b> Ob blažoviči 115, Limbuš info@xtension.si T.: 02/252 68 07</p>	 <p><b>GORENSKA TELEVIZIJA</b> P.P. 181, Oldhamska cesta 1A 4000 Kranj T.: 04/ 233 11 55 info@tele-tv.si, www.tele-tv.si</p>	 <p><b>VTV - VAŠA TELEVIZIJA</b> Žarova 10, Velenje tel.: 03/ 898 60 00, fax: 03/ 898 60 20 vttv.studio@iol.net, www.vttvstudio.com</p>
 <p><b>TV ŠIŠKA</b> Kebetova 1, Ljubljana tvsiska@kabelnet.si T.: 01/505 30 53</p>	 <p><b>INFOJOTA</b> Informacijski kanal Ajdovščina infojota@email.si gsm: 040 889 744</p>	 <p><b>TELEVIZIJA MEDVODE</b> Cesta kom. Staneta 12, 1215 Medvode T.: 01/361 95 80, F: 01/361 95 84</p>
		 <p><b>TELEVIZIJA ETV</b> Loke pri Zagorju 22, 1412 Kisovec GSM: 041-779-390 televizija@etv-hd.si, www.etv-hd.si</p>
		 <p><b>TELEVIZIJA VAŠ KANAL</b> Podbevska 12, Novo mesto T.: 07/39 30 860, www.vaskanal.com</p>
		 <p><b>NOVA GORICA</b> Gregorčičeva 13, Dornberk T.: 05/335 15 90, F.: 05/335 15 94 info@vitel.si, www.vitel.si</p>



# Ali so vaši podatki varni?

SVET TEMELJI NA PODATKIH. VSAKA INTERAKCIJA, OD SPLETNEGA NAKUPA DO UPORABE MOBILNE APLIKACIJE, USTVARJA DIGITALNE SLEDI, KI IMAJO ZA POSAMEZNIKA IN ORGANIZACIJE VELIKO VREDNOST.

Prav zato postajata varnost podatkov in njihova ustrežna hramba ena ključnih tem sodobne družbe. Ne gre več zgolj za tehnično vprašanje, temveč za kombinacijo tehnologije, zakonodaje, organizacije in človeškega vedenja.

Kibernetska varnost je danes neločljivo povezana s poslovno stabilnostjo, zaupanjem uporabnikov in celo nacionalno varnostjo. Organizacije, ki podatkov ne znajo zaščititi, se lahko soočajo s finančnimi izgubami in tudi z izgubo ugleda, kar je pogosto še težje popraviti.

## EVOLUCIJA KIBERNETSKIH GROŽENJ

V zadnjih letih so se kibernetske grožnje močno razvile. Napadi niso več naključni ali amaterski, temveč so organizirani, ciljani in pogosto finančno motivirani. Med najpogostejšimi oblikami napadov ostajajo izsiljevalski virusi, kraja identitet ter napadi na dobavne verige, ki omogočajo vdor v večje sisteme prek šibkejših partnerjev. Posebej pomembno je, da se je težišče napadov premaknilo na identiteto uporabnika. Namesto napada na infrastrukturo napadalci pogosto ciljajo prijavne podatke, saj ti omogočajo nepo-

sreden dostop do sistemov. To potrjujejo tudi sodobne analize, ki izpostavljajo identiteto kot enega ključnih vektorjev napada v podjetjih.

Napadi z izsiljevalskimi programi ostajajo ena največjih groženj. Ti napadi ne šifrirajo le podatkov,



temveč pogosto vključujejo tudi krajo informacij, kar pomeni dvojno izsiljevanje. Organizacije so se tako prisiljene odločati med plačilom odkupnine in tveganjem razkritja občutljivih podatkov.

Še pred nekaj leti smo phishing prepoznali po slabi slovenščini in sumljivih povezavah. Danes so napadalci precej bolj prefinjeni. Umetna inteligenca (UI) je postala glavno orodje kibernetskih kriminalcev. S pomočjo orodij za kloniranje glasu in generiranje videa (deepfake) lahko napadalci simulirajo klic vašega direktorja ali celo družinskega člana. Primer: Prejmete video klic bližnje osebe, ki pravi, da je v težavah in potrebuje nujen prenos sredstev. Videti je kot ona, slišati je kot ona, a v resnici gre za algoritem.

Hekerji ne sedijo več za zasloni in ne ugibajo vaših gesel ročno. Uporabljajo botnete, ki jih poganja UI. Ti v milisekundi preizkusijo milijone kombinacij ali iščejo luknje v programski opremi, še preden jih razvijalci sploh opazijo.

## VLOGA ZAKONODAJE IN REGULATIVE

Evropska unija je v zadnjih letih močno okrepila zakonodajni okvir na področju varnosti podat-

kov. Direktiva NIS2 predstavlja enega najpomembnejših korakov v tej smeri, saj razširja obveznosti kibernetike varnosti na širši krog organizacij in uvaja strožje zahteve glede upravljanja tveganj ter poročanja o incidentih.

NIS2 ni zgolj formalnost, temveč zahteva sistematičen pristop k varnosti. Organizacije morajo aktivno prepoznavati tveganja, uvajati zaščitne ukrepe in imeti jasno opredeljene postopke za odzivanje na incidente. Direktiva je bila prenesena tudi v slovenski pravni red z Zakonom o informacijski varnosti, ki dodatno poudarja odgovornost podjetij za zaščito digitalnega okolja. Poleg tega evropske pobude vse bolj poudarjajo zaščito kritične infrastrukture, dobavnih verig in sektorjev, kot je zdravstvo, kjer so posledice kibernetičnih napadov lahko neposredno povezane z življenjem ljudi.

Za vsakdanjo prakso za podjetja to pomeni: (1) podatke morate razvrstiti in jim določiti roke hrambe, (2) vpeljati šifriranje in dobro upravljanje ključev, (3) za oblak razumeti model deljene odgovornosti in najpogostejše pasti, (4) imeti preverjene varnostne kopije z jasnimi cilji RTO/RPO, (5) zaščititi identitete (MFA, najmanjša pooblastila) in končne naprave, ter (6) imeti pripravljen načrt odziva na incidente, ker roki za obveščanje niso "nekega dne", ampak so pogosto merjeni v urah.

### HRAMBA PODATKOV KOT TEMELJ ODPORNOSTI

Varnost podatkov ni mogoča brez ustrezne hrambe. Hramba podatkov pomeni več kot le shranjevanje informacij. Gre za zagotavljanje njihove razpoložljivosti, celovitosti in zaupnosti skozi celoten življenjski cikel.

Eden ključnih konceptov na tem področju je odpornost. Organizacije morajo biti pripravljene na scenarije, v katerih pride do izgube podatkov



ali napada. To pomeni, da morajo imeti vzpostavljene varnostne kopije, ki so ločene od primarnega sistema in zaščitene pred napadalci. Pomembno je tudi razumevanje, da hramba podatkov ni statičen proces. Podatki se spreminjajo, dopolnjujejo in brišejo, zato mora biti tudi sistem hrambe prilagodljiv. V praksi to pomeni kombinacijo lokalnih in oblaknih rešitev, ki skupaj zagotavljajo večjo odpornost.

### OBLAČNE TEHNOLOGIJE IN NOVA TVEGANJA

Uporaba oblaka je postala standard, vendar pri naša tudi nove izzive. Eden ključnih konceptov pri oblakni varnosti je deljena odgovornost. Ponudnik oblaka skrbi za infrastrukturo, medtem ko je uporabnik odgovoren za varnost podatkov in konfiguracijo sistema.

Napake pri konfiguraciji so eden najpogostejših vzrokov za uhajanje podatkov. Nepravilno nastavljeni dostopi lahko povzročijo, da so podatki javno dostopni, kar predstavlja resno varnostno

tveganje. Poleg tega oblak povečuje kompleksnost okolja. Podatki so lahko razpršeni po različnih lokacijah, kar otežuje nadzor in upravljanje. Zato postaja vse pomembnejši koncept ničelnega zaupanja, ki predpostavlja, da noben uporabnik ali sistem ni samodejno zaupanja vreden.

### VLOGA UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI

Umetna inteligenca postaja pomemben dejavnik tako na strani napadalcev kot na strani obrambe. Na eni strani omogoča avtomatizacijo napadov in bolj sofisticirane tehnike, na drugi pa izboljšuje zaznavanje groženj in odzivanje nanje. Sodobni varnostni sistemi uporabljajo umetno inteligenco za analizo velikih količin podatkov in prepoznavanje nenavadnih vzorcev. To omogoča hitrejšo odkrivanje napadov in zmanjšuje čas odziva. Vendar pa uporaba umetne inteligence odpira tudi nova vprašanja,

**IMATE TEŽAVE S KRIŽEM,  
BOLEČINE V VRATU, ZAPESTJU?**



**MI IMAMO REŠITEV ... PREVERITE  
FIZIOTERAPIJA IN  
ALTERNATIVNE METODE ZDRAVLJENJA**



VITA SPA D.O.O. | WWW.VITA-SPA.SI | INFO: 031 807 784  
KAPUCINSKI TRG 9 | ŠKOFJA LOKA - POSLOVNI DEL HOTELA LONČA ŠKOFJA LOKA





predvsem na področju zasebnosti in zlorabe tehnologije. Zato je pomembno, da se razvoj teh rešitev spremlja tudi z ustreznimi etičnimi in pravnimi okviri.

### ČLOVEŠKI DEJAVNIK KOT NAJŠIBKEJŠI ČLEN

Ne glede na tehnološki napredek ostaja človek najšibkejši člen v verigi kibernetске varnosti. Napadi, kot so phishing in socialni inženiring, izkoriščajo človeško nepazljivost in pomanjkanje znanja. Izobraževanje zaposlenih je zato eden ključnih elementov varnostne strategije. Organizacije morajo vlagati v ozaveščanje in usposabljanje, saj lahko že ena napačna odločitev povzroči resne posledice.

Pomembno je tudi, da se varnost ne dojema kot ovira, temveč kot sestavni del poslovanja. Le tako lahko postane del organizacijske kulture in ne zgolj formalna zahteva.

### ARHITEKTURA ZERO TRUST (NIČELNO ZAUPANJE)

Danes pri kibernetски varnosti prevladuje koncept Zero Trust. Njegovo glavno pravilo je: Nikoli ne zaupaj, vedno preveri.

Vsaka naprava, vsak uporabnik in vsaka povezava se mora nenehno identificirati.

Tudi če ste že prijavljeni v svoj e-poštni predal, bo sistem ob poskusu dostopa do občutljivih datotek ponovno zahteval potrditev identitete (npr. s prstnim odtisom ali skeniranjem obraza).

### ODZIVANJE NA INCIDENTE IN DIGITALNA FORENZIKA

Kljub vsem preventivnim ukrepom popolna zaščita ni mogoča. Zato je ključno, da imajo organizacije pripravljene načrte za odzivanje na incidente. Ti načrti določajo, kako prepoznati napad, kako omejiti škodo in kako obnoviti delovanje sistema.

Sodobni pristopi k odzivanju temeljijo na hitrem zaznavanju, analizi in odpravi grožnje. Pri tem igra pomembno vlogo digitalna forenzika, saj omogoča razumevanje, kako je do napada prišlo in kako ga v prihodnje preprečiti.



Evropska unija je sprejela tudi načrte za obvladovanje kibernetских kriz, ki poudarjajo sodelovanje med državami in organizacijami ter koordiniran odziv na večje incidente.

### KRIPTOGRAFIJA IN KVANTNA GROŽNJA

Kriptografija ne predstavlja več le neprebojnega ščita, temveč postaja bojišče med klasično zaščito in vzponom kvantnih računalnikov. Večina današnjega digitalnega zaupanja, od spletnega bančništva do varnih protokolov HTTPS, temelji na asimetričnem šifriranju RSA, ki svojo varnost črpa iz nezmožnosti klasičnih računalnikov, da bi hitro razcepili ogromna števila. Kvantni računalniki s pomočjo Shorovega algoritma in kvantnih bitov to matematično oviro premagajo v nekaj minutah, kar postavlja rok trajanja na našo celotno digitalno preteklost.

Posebno tveganje predstavlja strategija, znana kot ukradi zdaj, dešifriraj pozneje, kjer napadalci in državni akterji že danes prestrezajo in shranjujejo ogromne količine šifriranih podatkov, od zasebnih sporočil do zdravstvenih kartonov. Čeprav teh informacij trenutno ne morejo prebrati, bodo postale popolnoma izpostavljene tisti trenutek, ko bo kvantna tehnologija dosegla kritično točko moči. Kot odgovor na to grožnjo v letu 2026 prehajamo na standarde post-quantne kriptografije, ki temeljijo na matematiki rešetk in so odporni na moč kvantnih strojev. Pri izbiri sodobnih storitev je zato nujno iskati ponudnike, ki že uporabljajo hibridne protokole, saj ti združujejo preverjeno klasično varnost z novo, na kvantne napade odporno zaščito.

Vzporedno s kriptografsko bitko se odvija gospodarska transformacija, kjer so vaši podatki postali osnovna valuta za izgradnjo tako imenovanih digitalnih dvojčkov. V letu 2026 niste le uporabnik,

temveč vir surovine za podatkovne posrednike, ki s pomočjo umetne inteligence analizirajo vsak vaš srčni utrip, porabo energije in finančno transakcijo. Ti napovedni modeli ne služijo le oglaševanju, temveč lahko neposredno vplivajo na vaše zavarovalne premije ali kreditno sposobnost, ne da bi se vi tega sploh zavedali.

Za ohranitev osebne integritete v takšnem okolju osnovni ukrepi, kot so gesla, niso več dovolj, zato se uveljavljajo naprednejša orodja digitalne higijene. Tehnologija dokazov z ničelnim razkritjem omogoča, da storitvam dokažete svojo identiteto ali starost, ne da bi jim dejansko razkrili svoje osebne podatke. Hkrati decentralizirana identiteta uporabnikom vrača lastništvo nad ključi do njihovih profilov, s čimer se zmanjšuje odvisnost od velikih tehnoloških platform, ki nenehno trgujejo z našo zasebnostjo.

Celovito obrambo v globino dopolnjujejo še tehnični popravki, kot je šifriranje DNS poizvedb, ki ponudnikom interneta preprečuje sledenje vašemu obisku spletnih domen, ter uporaba e-poštnih "aliasov" za preprečevanje povezovanja vaših digitalnih sledi.

### PRIHODNOST VARNOSTI PODATKOV

Varnost podatkov bo v prihodnje še pomembnejša, saj se digitalizacija nadaljuje. Internet stvari, pametna mesta in napredni industrijski sistemi povečujejo količino podatkov in hkrati širijo napadalno površino.

Hkrati se povečuje tudi pomen dobavnih verig, kjer lahko napadalci izkoristijo šibke točke pri partnerjih. Evropska politika zato vse bolj poudarja potrebo po varnosti celotnega ekosistema, ne le posameznih organizacij.

V prihodnje lahko pričakujemo tudi strožjo regulativo, večjo avtomatizacijo varnostnih procesov in večji poudarek na odpornosti sistemov.

# EXCLUSIVE 25<sup>let</sup>

Za moške, ki cenijo izjemen, brezčasen slog



## NOVA SERIJA PLATINUM



### **Ekskluzivno za naročnike revije AVTOFOKUS!**

Jubilejna, omejena serija ob 25. obletnici revije  
s kronografom zasebne znamke Sportive Swiss Made.

Platirano ohišje iz nerjavečega jekla • K1 ekstra kaljeno mineralno steklo  
s safirnim premazom • Vodoodpornost do 100M/10ATM • Švicarski  
kronografski mehanizem 1/10 • Kaliber: Ronda Quartz Cal. 5040.D • Premer  
ohišja: 42 mm • Debelina ohišja: 12 mm • 2-letna garancija

Ob dvoletni naročnini (s 15 % popustom): **100,30 €**  
in doplačilo za uro **148 €** (Vrednost ure je 400 €)\*



Za ekskluzivno ponudbo  
slikajte QR kodo. Informacije  
in naročila tudi na: 01/236 10 00

\* Ponudba velja do porabe zalog.



INFO HIŠA D.O.O.

# Manj je več: zakaj minimizacija podatkov ščiti uporabnike in podjetja

Z UPOŠTEVANJEM NAČELA MINIMIZACIJE PODATKOV NE LE SLEDIMO ZAKONODAJI, TEMVEČ USTVARJAMO VARNEJŠE DIGITALNO OKOLJE, KJER JE ZBIranJE PODATKOV OMEJENO LE NA NUJNO POTREBNO.

Načelo minimizacije podatkov s tem pomaga preprečevati nepotrebno izpostavljenost, krepi varnost informacij in zmanjšuje verjetnost kršitev ali zlorab.

## ZAŠČITA OSEBNIH PODATKOV JE BISTVENEGA POMENA

V digitalnem svetu, kjer podatki postajajo ključna valuta, je zaščita osebnih podatkov bistvenega pomena za zaupanje uporabnikov in varnost informacij. Splošna uredba o varstvu podatkov (GDPR) med ključnimi načeli obdelave izpostavlja načelo minimizacije, ki določa, da se osebni podatki zbirajo in obdelujejo le v obsegu, ki je nujno potreben za doseganje jasno določenega, zakonitega in legitimnega namena obdelave.

Omejevanje količine in vrste podatkov zmanjšuje tveganje za kršitve zasebnosti, preprečuje nepotrebno izpostavljenost in omogoča učinkovitejšo upravljanje informacij ter nižje stroške hrambe.

## URAVNOTEŽENA MINIMIZACIJA: ZBRATI DOVOLJ, A NE PREVEČ

Učinkovita implementacija načela minimizacije vključuje temeljit pregled vseh procesov zbiranja in obdelave podatkov ter natančno določitev podatkov, ki so ključni za doseg določenega namena. Pomemben del izvajanja minimizacije so tehnični in organizacijski ukrepi, kot so poenostav-

ljeni obrazci za zbiranje podatkov, anonimizacija ali psevdonomizacija, kjer je to mogoče, ter omejitve dostopa do podatkov le na osebe, ki jih potrebujejo za svoje delo. Na ta način organizacije zagotavljajo, da se obdelujejo le podatki, ki so nujno potrebni za določen namen.

Vendar pa je pri minimizaciji potrebno ohraniti ravnotežje. Prekomerno omejevanje zbiranja podatkov lahko vodi do tega, da organizacije ne zberejo dovolj informacij za nemoteno izvajanje delovnih procesov ali izpolnjevanje zakonskih zahtev, kar lahko povzroči operativne težave ali neizpolnjevanje obveznosti do uporabnikov in regulatorjev. Pravilno izvajanje minimizacije zato zahteva tehten pregled, kateri podatki so res nujni za namen obdelave, in katera omejitev bi lahko ogrozila delovanje ali skladnost z zakonodajo.

## MINIMIZACIJA KOT STRATEŠKA PREDNOST

Načelo minimizacije podatkov ni zgolj pravna zahteva, temveč tudi strateška prednost. Organizacije, ki ga dosledno upoštevajo, gradijo zaupanje uporabnikov, povečujejo preglednost svojih procesov in krepijo digitalno varnost. Omejevanje obsega podatkov prispeva k boljši zaščiti občutljivih informacij, optimizaciji notranjih procesov in zmanjšanju tveganja za kršitve ali zlorabe.

V praksi to pomeni, da manj podatkov resnično pomeni več – več varnosti, več zaupanja in več odgovornosti pri obdelavi osebnih podatkov.

Minimizacija podatkov postaja temelj trajnostne in zaupanja vredne digitalne prisotnosti, ki koristi uporabnikom, ponudnikom storitev in širši družbi.

## 12. KONFERENCA PRIVACY DAYS

Kako načelo minimizacije in druga načela Splošne uredbe učinkovito vključiti v svoje procese in druge aktualne tematike s področja varstva osebnih podatkov in informacijske varnosti, bodo podrobneje obravnavane na 12. konferenci Privacy Days, ki jo organizirata Info Hiša in Akademija Finance. Poseben poudarek bo namenjen tudi vplivu umetne inteligence na varstvo osebnih podatkov, saj uporaba naprednih tehnologij odpira nova vprašanja glede zakonite, transparentne in odgovorne obdelave podatkov. Več informacij o programu in prijavi je na voljo na spletni strani [privacy-days.com](https://privacy-days.com). (P.R.)



Info hiša d.o.o.

Likozarjeva ulica 14, 1000 Ljubljana

[www.info-hisa.si](https://www.info-hisa.si)

[info@info-hisa.si](mailto:info@info-hisa.si) | (01) 235 50 36

**12.** DNEVI PRAVA ZASEBNOSTI IN VAROVANJA INFORMACIJ  
16.-17. APRIL 2026  
HOTEL JAMA, POSTOJNA

**SKLADNOST z IN brez UI**

AKADEMIJA Finance | InfoHiša

DELINEA

# Digitalni ključni vašega podjetja: Kako z Delineo ustaviti vdore in prihraniti čas

UPRVLJANJE DOSTOPOV DANES NE SME BITI VEČ "IT PROBLEM", AMPAK STRATEŠKA ODLOČITEV UPRAVE, KI ŽELI ZAŠČITITI SVOJE PREMOŽENJE IN ZAGOTOVITI NEMOTENO POSLOVANJE V DIGITALNI DOBI.

"V preteklosti je bila kibernetika varnost podobna gradnji visokih zidov okoli pisarne. Danes pa ti zidovi ne obstajajo več, saj zaposleni delajo od koder koli, podjetja pa uporabljajo storitve v oblaku. Napadalci se ne trudijo več "prebiti" v vaš sistem; preprosto se vanj prijavijo z ukradenimi gesli. Kar 80 % vseh uspešnih vdorov se začne prav z zlorabo t. i. privilegiranih računov, torej tistih, ki imajo ključne do vaših najpomembnejših podatkov," pojasnjuje današnje varnostno-informacijsko razmere strokovnjak Dragan Ignjić iz podjetja Our Space Appliances.



## KJE PODJETJA NAJBOLJ BOLJ?

Ena največjih težav, s katerimi se danes soočajo podjetja in računalniški operaterji, je kaos pri upravljanju gesel, saj številne organizacije svoje dostope še vedno vodijo ročno, pogosto celo v izjemno nevarnih in neučinkovitih Excelovih tabelah. Poleg ljudi v sodobnih informacijskih sistemih deluje tudi vse več t. i. nevidnih delavcev, kot so strojni računi in AI agenti, ki po številu močno presegajo človeške uporabnike. Ti nečloveški akterji pogosto razpolagajo z obsežnimi, včasih celo "božanskimi" pooblastili, vendar kljub svoji moči pogosto ostajajo brez ustreznega nadzora in povsem izven dosega osrednjih varnostnih politik.



Ignjić opozarja, da če "napadalec ukrade te 'digitalne ključne', se lahko neovirano premika po vašem omrežju, ukrade podatke ali sproži izsiljevalski virus, kar podjetje stane, glede na rezultate interne Delinea raziskave iz letošnjega februarja, povprečno 5 % letnih prihodkov podjetja."

## PAMETNI TREZOR, KI DELA NAMESTO VAS

Rešitve podjetja Delinea, kot sta Secret Server in Delinea Platform, delujejo kot inteligentni digi-

talni varnostnik, saj zagotavljajo centralizirano in avtomatizirano avtorizacijo za vse vrste identitet. Namesto da bi si morali operaterji zapomniti zapletena gesla, platforma varno shrani vse digitalne ključne in poverilnice v šifriran, centraliziran trezor, do katerega imajo na podlagi strogih politik dostop le pooblaščen uporabniki. Sistem nato samodejno izvaja rotacijo gesel, s čimer doseže, da morebitni ukradeni podatki za napadalce postanejo neuporabni, hkrati pa se zmanjša tveganje človeških napak pri upravljanju dostopov. Poleg tega Delinea neprekinjeno snema in nadzoruje delo vseh privilegiranih uporabnikov, kar deluje podobno kot varnostne kamere v banki.

## POSLOVNI IN FINANČNI UČINKI – VARNOST, KI SE IZPLAČA

Za vodstvo podjetja Delinea ne predstavlja zgolj stroška, temveč strateško naložbo z izjemno hitrim povratkom in merljivimi poslovnimi učinki na več nivojih. Zaradi visoke stopnje inteligentne avtomatizacije platforma zahteva kar 90 % manj virov za upravljanje kot najbližje konkurenčne rešitve, kar IT-skrbnikom drastično skrajša čas za rutinsko delo in jim omogoči popolno osredotočenost na razvojne projekte. V nasprotju s tradicionalnimi kompleksnimi sistemi, ki zahtevajo dolgotrajno uvajanje, Delinea omogoča izjemno hitro pot do varnosti, saj se rešitev namesto v mesecih v celoti vzpostavi v le nekaj tednih. "Ta učinkovitost se neposredno odraža tudi pri revizijah, kjer se dolgotrajna in mučna

priprava na varnostne preglede (npr. za direktivo NIS2 ali standarde HIPAA in GDPR) skrajša z več mesecev na vsega nekaj dni, kar organizaciji prinese 'zeleno kljukico' pri revizorjih brez nepotrebne hrupa v ozadju," dodaja Ignjić, ki je bil med drugim nekaj let zaposlen v podjetju Delinea kot višji svetovalec podjetjem s tudi več kot 100.000 zaposlenimi.

V Sloveniji podjetjem pri uvajanju Delinea rešitev in kasnejši podpori pomaga strateški partner Our Space Appliances, ki je kot edino podjetje v Sloveniji usposobljeno za izvajanje Delinea Professional Services v regiji EMEA. Professional Services zajemajo svetovanje, načrtovanje in implementacijo Delinea rešitev, razvoj prilagojenih integracij z obstoječimi informacijskimi sistemi ter usposabljanje strank za učinkovito upravljanje in uporabo rešitev po principu »train-the-trainer«. Vse to zagotavlja, da je prehod na sodoben in varen način dela hiter, strokovno voden in prilagojen lokalnim zahtevam. (P.R.)



### Our Space Appliances, d.o.o.

Stegne 11c, 1000 Ljubljana, Slovenija

• Tel: +386 (0)1 810 03 43

• E-pošta: info@ourspace.si

[www.ourspace.si](http://www.ourspace.si)



# INTERVJU: Siniša Kovač, strokovnjak za kibernetično varnost, Check Point »Velikost podjetja ni več zaščita«

KIBERNETSKI NAPADI SO HITREJŠI, PAMETNEJŠI IN BOLJ CILJANI KOT KADARKOLI PREJ. OBRAMBA MORA BITI ŠE HITREJŠA.

Digitalizacija, prehod v oblak in razvoj umetne inteligence prinašajo številne priložnosti, hkrati pa tudi nova tveganja, ki jih podjetja ne smejo podcenjevati. O tem, kako se spreminja kibernetična ogroženost, kateri so največji varnostni izzivi ter kako se jim lahko podjetja učinkovito zoperstavijo, smo se pogovarjali s Sinišo Kovačem (Territory Manager Slovenia & Croatia, Check Point), strokovnjakom s področja kibernetične varnosti.

## Kako se je v zadnjih letih spremenila kibernetična ogroženost podjetij v Sloveniji? Opažate specifične trende?

V zadnjih letih se je kibernetična ogroženost slovenskih podjetij izrazito povečala. Napadi so postali ciljani, organizirani in finančno motivirani, napadalci pa delujejo profesionalno in dobro poznajo šibke točke. Najbolj izstopajo izsiljevalski napadi, kjer napadalci poleg šifriranja podatkov grozijo tudi z njihovo objavo, kar pomeni operativna in reputacijska tveganja.

V porastu so tudi napadi na dobavne verige, kjer napadalci prek slabše zaščitene partnerjev dostopajo do večjih organizacij, zlasti v proizvodnji in IT-storitvah. Srednja in vzhodna Evropa sodita med regije z najhitrejšo rastjo napadov, pogosto pa so tarča srednje velika podjetja.

Opažamo tudi več napadov, povezanih z geopolitičnimi napetostmi, predvsem DDoS na javne institucije. Ključno sporočilo je, da velikost podjetja ni več zaščita – nujni so večplastna varnost, izobraževanje zaposlenih in pripravljen odzivni načrt.

## Kateri so največji varnostni izzivi pri prehodu v hibridna in multi-cloud okolja?

Prehod v oblak prinaša številne izzive, predvsem zaradi večje kompleksnosti. Največji problem je pomanjkanje enotnega nadzora, saj ima vsak ponudnik svoje politike in orodja, kar ustvarja varnostne vrzeli. Pogost vzrok incidentov so tudi napačne konfiguracije, kjer že ena napaka lahko izpostavi podatke.

Pomemben izziv so identitete in dostopi – brez centralnega upravljanja in večfaktorske avtentikacije se tveganje močno poveča. Podjetja pogosto spregledajo, da je odgovornost v oblaku deljena: ponudnik skrbi za infrastrukturo, podjetje pa za podatke in nastavitve. Dodaten problem sta pomanjkanje kadrov in znanja. Zato so ključni centraliziran nadzor, avtomatizacija in stalno spremljanje groženj. Oblak prinaša prednosti, vendar mora biti varnost enakovreden del strategije.

## Kako se spreminja vloga IT-oddelkov?

Vloga IT in varnostnih ekip se je premaknila iz tehnične podpore v strateškega partnerja poslovnega vodstva. Namesto reaktivnega odzivanja se osredotočajo na proaktivno upravljanje tveganj, spremljanje groženj, avtomatizacijo in sodelovanje z drugimi oddelki. Varnost postaja del celotnega poslovnega ekosistema. Pomembna je tudi zaščita v hibridnih okoljih, kar zahteva nova znanja in enotno strategijo. Povečuje se pomen izobraževanja zaposlenih, saj človeški faktor ostaja ključna ranljivost. Spreminja se tudi profil kadrov – potrebni so strokovnjaki, ki razumejo tehnologijo in poslovanje ter znajo komunicirati z vodstvom. IT se tako iz izvajalca spreminja v svetovalca.

## Kako vidite vlogo umetne inteligence?

Umetna inteligenca (UI) je danes ključni dejavnik na obeh straneh. Napadalcem omogoča hitreše, bolj personalizirane in težje zaznavne napade, od naprednega phishinga do avtomatiziranega iskanja ranljivosti. Hkrati pa UI bistveno izboljšuje obrambo, saj omogoča zaznavanje anomalij, napovedovanje tveganj in avtomatsko blokiranje napadov. Za podjetja so ključni trije koraki: avtomatizacija, saj ročno upravljanje ni več dovolj; konsolidacija rešitev, ker več orodij pomeni več vrzeli; ter izobraževanje zaposlenih. UI tekma se bo še stopnjevala, zato bodo najbolj uspešna podjetja tista, ki



Siniša Kovač, Territory Manager Slovenia & Croatia, Check Point

bodo pravočasno vlagala v znanje in pametne tehnologije.

## Ali lahko srednje velika podjetja zgradijo robustno varnost brez visokih stroškov?

Da. Ključ ni v količini orodij, temveč v strategiji. Konsolidacija rešitev zmanjšuje kompleksnost, stroške in tveganja. Avtomatizacija omogoča učinkovito zaščito tudi z omejenimi kadri. Pomembna je prioritizacija – zaščititi je treba predvsem kritične sisteme in podatke. Izobraževanje zaposlenih je cenovno dostopno, a zelo učinkovito. Prednost srednje velikih podjetij je tudi agilnost, saj lahko hitreje uvajajo spremembe. Z ustreznim pristopom lahko dosežejo visoko raven varnosti brez nesorazmernih investicij.

## Kako ocenjujete partnerstvo med Check Pointom in Ingram Micro?

Partnerstvo je zelo dobro uigrano in pomembno za slovenski trg. Check Point prinaša vrhunsko tehnologijo in globalno znanje, Ingram Micro pa lokalno prisotnost, podporo in razumevanje trga. Ne deluje le kot distributer, temveč kot podpora partnerjem pri izobraževanju, načrtovanju in implementaciji rešitev. To podjetjem omogoča dostop do globalnih rešitev z lokalno podporo, kar je ključno za hitro odzivanje in zaupanje. Kombinacija globalne moči in lokalne zanesljivosti je ena ključnih prednosti tega partnerstva.

(P.R.)




**Ingram Micro Ljubljana, d.o.o.**  
Gmajna 10  
1236 Trzin - Ljubljana

T: +386 1 600 25 80  
checkpointteamslovenia@ingrammicro.com

W: si.ingrammicro.eu

# POMLADNI KLIK DO DOBRE KNJIGE, več kot 30 naslovov...



22 €



12 €



5 €



18 €



8 €

pomladna ponudba knjig na  
[www.tzs.si](http://www.tzs.si) ter na tel: **01 479 02 24**





SOPHOS MDR

# Vaše podjetje pod budnim očesom strokovnjakov: zakaj izbrati Sophos MDR?

AVTOMATIZIRANI IN CILJANI KIBERNETSKI NAPADI NA PODJETJA SO POSTALI STALNICA, NAPADALCI PA NE PRIZANAŠAJO NITI SLOVENSKIM ORGANIZACIJAM.

V času, ko napadalci izkoriščajo napredno umetno inteligenco, prestrezajo gesla in zlorablajo neodpravljene ranljivosti, pasivna zaščita preprosto ne zadošča več. Rešitev, ki ji danes zaupa že več kot 36.000 organizacij po svetu in ki postavlja nove standarde na področju varnosti, je Sophos MDR.

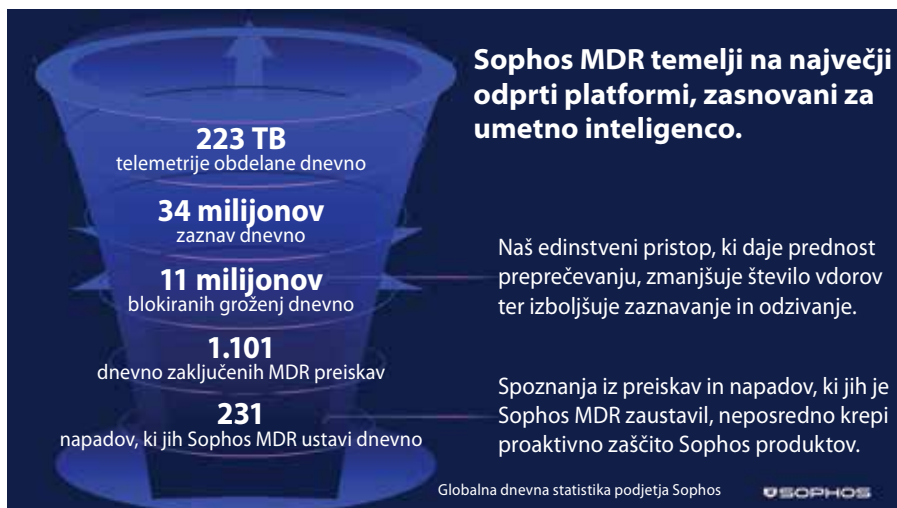
## TEHNOLOGIJA, PODPRTA S ČLOVEŠKIM ZNANJEM

Sodobna kibernetška varnost se sooča z velikim izzivom – akutnim pomanjkanjem strokovnega kadra. Študija ISC2 Cybersecurity Workforce Study 2024 razkriva, da bi za popolnitev vrzeli na svetovnem trgu potrebovali kar 4,76 milijona strokovnjakov. To pomanjkanje pušča podjetja ranljiva, zlasti v kritičnih trenutkih.

Sophos, ki že več kot štiri desetletja narekuje trende v industriji, s svojo rešitvijo ne ponuja le tehnologije, temveč tudi elitno ekipo več kot 500 analitikov po vsem svetu, ki za vas delujejo neprekinjeno, 24 ur na dan in 7 dni v tednu. Da gre za eno najbolj zaupanja vrednih MDR-storitev na svetu, potrjujejo tudi uporabniki na platformi Gartner® Peer Insights™, kjer Sophos dosega oceno 4,9 od 5,0.

## ODZIVNOST, KI ŠTEJE V MINUTAH

V svetu kibernetških groženj sekunde pogosto pomenijo razliko med nemotenim poslovanjem in drago sanacijo škode. Sophos MDR izstopa po hitrosti odziva: povprečni čas zaznave grožnje znaša manj kot minuto, strokovna preiskava pa se začne v manj kot 25 minutah. Za razliko od ponudnikov, ki zgolj opozarjajo na grožnje, Sophosovi strokovnjaki te aktivno omejijo in nevtralizirajo. Ugotovitve najnovejšega poročila Sophos Active Adversary Report 2026 dodatno potrjujejo, zakaj je hiter in stalen nadzor danes nu-



jen. Sophos je ugotovil, da se 88 % napadov z izsiljevalsko programsko opremo in 79 % dejani iznosa podatkov zgodi zunaj običajnega delovnega časa. Hkrati je povprečni čas zadrževanja napadalca v okolju padel na tri dni, po vstopu v organizacijo pa ti v povprečju potrebujejo le 3,4 ure, da dosežejo strežnik Active Directory. To pomeni, da si podjetja preprosto ne morejo več privoščiti varnosti, ki je odvisna le od delovnika interne varnostne ekipe.

## NAPADI NA IDENTITETE V OSPREDJU

Eden najpomembnejših poudarkov poročila Sophos Active Adversary Report 2026 je premik težišča napadov na področje identitet. Kar 67 % vseh incidentov, ki so jih obravnavale ekipe Sophos IR in MDR, je bilo povezanih z napadi na identitete, kot so zloraba ukradenih poverilnic, brute-force napadi, phishing ter slabo zaščiteni sistemi za upravljanje identitet. Sophos ob tem opozarja, da napadalci za uspešen začetni dostop vse pogosteje ne potrebujejo več posebej sofisticiranih tehnik, saj jim pot v okolje pogosto odprejo že veljavni uporabniški računi in pomanjkljivo zaščiteni prijavni mehanizmi. V 59 % obravnavanih primerov večfaktorska avtentikacija sploh ni bila prisotna, kar jasno kaže, da je zaščita identitet danes eden ključnih temeljev učinkovite kibernetške obrambe.

To je tudi eden ključnih razlogov, da je storitev, kot je Sophos MDR, bistveno več kot zgolj spremljanje opozoril. Gre za aktivno iskanje znakov

kompromisa, povezovanje dogodkov iz različnih virov, hitro razumevanje konteksta napada in takojšnje ukrepanje, še preden incident preraste v poslovno škodo.

## PRILAGODLJIVOST IN INTEGRACIJA

Sophos MDR deluje kot osrednje varnostno vozlišče, ki črpa podatke iz več kot 50 tehnoloških integracij. Podjetjem tako omogoča, da ohranijo obstoječe naložbe v rešitve proizvajalcev, kot so Microsoft, Fortinet, Cisco, Veeam in AWS, medtem ko Sophosovi analitiki te podatke povežejo v enoten varnostni ščit z vrhunsko vidljivostjo nad celotnim okoljem.

Sophosovi raziskovalci so v najnovejšem poročilu zaznali največje število aktivnih izsiljevalskih skupin doslej, pri čemer se povečujeta tako njihovo število kot raznolikost njihovih pristopov. To za podjetja jasno pomeni potrebo po varnostnem partnerju, ki zna podatke iz različnih sistemov povezati v jasno sliko in se nanjo tudi učinkovito odzvati.

## ZAKAJ SOPHOS MDR

Podjetja danes ne potrebujejo več zgolj še enega varnostnega orodja, temveč zanesljivega partnerja, ki združuje tehnologijo, izkušnje in neprekinjeno operativno odzivnost. Sophos MDR prinaša prav to: globalno ekipo strokovnjakov, hitro zaznavo in odziv, napredno zaščito identitet ter možnost, da iz obstoječega varnostnega okolja iztisnete največ. (P.R.)



**Distributer: Sophos d.o.o.**

Germova ulica 9, Novo mesto  
slovenija@sophos.si

07/393 5 600

[www.sophos.si](http://www.sophos.si)

DATAINFO.SI

# Visoke globe zaradi kršitev varstva osebnih podatkov v Sloveniji

DVA NEDAVNA PRIMERA KAŽETA, KAKO STROGO NADZORNI ORGANI SANKCIONIRAJO NEZAKONIT NADZOR ZAPOSLENIH IN POMANJKLJIVO OBVEŠČANJE POSAMEZNIKOV O OBDELAVI OSEBNIH PODATKOV.

V Sloveniji že skoraj 8 let velja Splošna uredba EU o varstvu podatkov (GDPR). Ta upravljavcem in obdelovalcem osebnih podatkov nalaga stroge obveznosti glede zakonite, pregledne in sorazmerne obdelave podatkov. Nadzor nad spoštovanjem teh pravil izvaja Informacijski pooblaščenec. Nedavna primera iz prakse jasno kažeta, da se je politika izrekanja glob Informacijskega pooblaščenca zelo spremenila in da sedaj ob ugotovljenih kršitvah izreka tudi visoke globe, zlasti kadar gre za posege v zasebnost posameznikov ali za pomanjkljivo obveščanje o obdelavi podatkov.

## NEZAKONIT NADZOR ZAPOSLENEGA JE STAL PODJETJE PREKO 70.000 EVROV

V prvem primeru je Informacijski pooblaščenec podjetju izrekel več kot 70.000 evrov globe zaradi nezakonitega nadzora službenega računalnika enega od zaposlenih. V postopku nadzora je bilo ugotovljeno, da je bila na računalnik nameščena programska oprema, ki je dalj časa neprekinjeno snemala in shranjevala vse aktivnosti zaposlenega.

Program ni beležil zgolj službenih opravil, temveč tudi številne zasebne podatke. Med drugim je beležil dostop do elektronske pošte Gmail, komunikacijo prek družbenih omrežij, podatke o obiskanih spletnih straneh ter informacije iz uporabniških profilov. Sistem je shranjeval tudi zvočne posnetke pogovorov, kar predstavlja še posebej intenziven poseg v zasebnost posameznika.

Nadzorni organ je ugotovil, da za takšno obdelavo osebnih podatkov ni obstajala nobena ustrezna pravna podlaga. Delodajalec namreč ni izkazal zakonitega interesa ali drugega pravnega temelja, ki bi upravičeval tako obsežen in trajen nadzor zaposlenega. S tem je bilo kršeno temeljno načelo zakonitosti obdelave osebnih podatkov, ki ga določa Splošna uredba o varstvu podatkov.

Odgovorna oseba podjetja mora zaradi kršitve plačati 4.000 evrov globe in sodno takso, podjetju pa je bila izrečena globa v višini 71.474 evrov ter dodatna sodna taksa, ki presega



7.000 evrov. Primer predstavlja jasno opozorilo delodajalcem, da nadzor na delovnem mestu ni neomejen in da mora biti vsak poseg v zasebnost zaposlenih utemeljen, sorazmeren in podprt z ustrezno pravno podlago.

## POMANJKLJIVO OBVEŠČANJE UDELEŽENCEV DOGODKA JE STALO PODJETJE PREKO 35.000 EVROV

V drugem primeru je Informacijski pooblaščenec kaznoval podjetje in njegovo odgovorno osebo zaradi kršitve obveznosti obveščanja posameznikov o obdelavi njihovih osebnih podatkov. Skupna kazen v tem primeru presega 35.000 evrov.

Ugotovljeno je bilo, da so se posamezniki na dogodek prijavljali prek spletnega obrazca, pri čemer niso prejeli vseh informacij, ki jih mora upravljavec zagotoviti ob zbiranju osebnih podatkov. Obrazec je vseboval zgolj splošno navedbo, da so podatki potrebni za izvedbo prireditve in da brez soglasja ne bodo uporabljeni za druge namene.

Manjkale pa so ključne informacije, ki jih zahteva 13. člen Splošne uredbe o varstvu podatkov. Udeleženci niso bili ustrezno obveščeni o tem, kdo je upravljavec njihovih osebnih podatkov, za kakšne konkretne namene se bodo podatki obdelovali, kako dolgo se bodo hranili ter katere pravice imajo posamezniki v zvezi z obdelavo njihovih podatkov.

Po presoji Informacijskega pooblaščenca je bila s tem kršena pravica posameznikov do obveščenoosti, ki predstavlja eno izmed temeljnih načel varstva osebnih podatkov. Transparentnost obdelave je namreč ključni element zaupanja med upravljavci in posamezniki. Odgovorna oseba po-

djetja je bila kaznovana s 600 evri globe, podjetju pa je bila izrečena globa v višini 34.951,04 evra ter dodatna sodna taksa v višini 3.495,10 evra.

## JASNO OPOZORILO UPRAVLJAVCEM OSEBNIH PODATKOV

Oba primera potrjujeta, da nadzorni organi v Sloveniji dosledno izvajajo določbe zakonodaje na področju varstva osebnih podatkov. Kršitve, ki se morda na prvi pogled zdijo administrativne ali organizacijske narave, lahko vodijo do zelo visokih finančnih sankcij.

Podjetja, organizatorji dogodkov in drugi upravljavci osebnih podatkov morajo zato posebno pozornost nameniti zakonitosti obdelave, spoštovanju načela sorazmernosti ter predvsem transparentnemu obveščanju posameznikov. Samo celovit in odgovoren pristop k varstvu osebnih podatkov lahko prepreči kršitve, ki lahko poleg finančnih posledic povzročijo tudi izgubo zaupanja javnosti in poslovnih partnerjev. Če želite to področje urediti učinkovito in brez nepotrebnih zapletov, vam lahko pomagajo strokovnjaki iz DATAINFO.SI – za brezplačen posvet jih lahko pokličete na 02 620 43 00 ali pišete na [info@datainfo.si](mailto:info@datainfo.si). (P.R.)

**DATAINFO.SI, d.o.o.**

02 620 43 00

[info@datainfo.si](mailto:info@datainfo.si)

<https://datainfo.si>



ANNI D.O.O., CENTER ZA KIBERNETSKO VARNOST

# Ne ugibajte, raje preverite, kako zanesljiva je vaša digitalna zaščita

## VARNOSTNI PREGLED IKT OKOLJA.

Digitalno okolje je danes temelj poslovanja. Večina procesov – od komunikacije in hrambe podatkov do izvajanja storitev – poteka v informacijskih sistemih. S tem pa narašča tudi izpostavljenost kibernetiskim tveganjem, ki postajajo vse bolj ciljana, napredna in poslovno motivirana. Napadi niso več omejeni na velika podjetja. Ravno nasprotno – mala in srednja podjetja ter javne ustanove so pogosto še bolj izpostavljene, saj imajo manj virov za sistematično upravljanje varnosti. Hkrati regulatorni okviri, kot so NIS2, ZInfV-1 in GDPR, zahtevajo jasno razumevanje tveganj in dokazljivo izvajanje zaščitnih ukrepov.

### TARČA SMO VSI

Ne glede na dejavnost ali velikost organizacije je vsak informacijski sistem potencialna tarča. Napadalci ne izkoriščajo le tehničnih ranljivosti, temveč tudi organizacijske pomanjkljivosti in človeške napake.

Posledice so lahko resne: od nedelovanja sistemov in izgube podatkov do finančne škode in izgube zaupanja. Vse pogostejše pa imajo incidenti tudi regulatorne posledice.

### NEVIDNA TVEGANJA ZAHTEVAJO PREVERJANJE

Kibernetiskih tveganj ne vidimo – sistemi lahko delujejo brezhibno, v ozadju pa obstajajo ranli-



vosti. Zato je redno preverjanje ključno. S preventivnim pristopom in ustrezno zaščito lahko organizacije bistveno zmanjšajo tveganja. Vendar varnost ni enkratni projekt, temveč proces, ki zahteva stalno prilagajanje.

### VARNOSTNI PREGLED KOT NUJEN KORAK

Pri kibernetiski varnosti velja preprosto pravilo: ne ugibajte, preverite. Varnostni pregled IKT okolja omogoča realen vpogled v stanje varnosti. Vključuje pregled infrastrukture, konfiguracij in dostopov ter identifikacijo ranljivosti. Rezultat so jasna priporočila za izboljšave, razvrščena glede na tveganje za poslovanje. Takšen pregled je primerljiv s tehničnim pregledom vozila – namenjen je pravočasnemu odkrivanju težav, preden povzročijo škodo.

### ČLOVEK OSTAJA KLJUČNI DEJAVNIK

Tehnologija sama po sebi ni dovolj. Zaposleni so pogosto prva točka napada, zato je njihovo zavedanje ključno. Z izobraževanjem in ozaveščanjem lahko organizacije bistveno zmanjšajo tveganja in okrepijo svojo odpornost.

### VARNOST KOT POSLOVNA ODLOČITEV

Kibernetiska varnost ni več zgolj IT vprašanje, temveč del odgovornega upravljanja. Organizacije, ki redno preverjajo svojo digitalno zaščito, lažje obvladujejo tveganja in izpolnjujejo regulatorne zahteve. Vprašanje zato ni več, ali preveriti stanje varnosti – temveč kako to narediti pravočasno in sistematično. Več informacij najdete na [www.varen.it](http://www.varen.it). (P.R.)



**CYBER  
SECURITY  
TEAM  
@ANNI**



#### Anni d.o.o.

Motnica 7a, Trzin,

T: 01/ 5800 800 • [info@varen.it](mailto:info@varen.it)

Toni JERŠIN • M 041 820 577

Matej PERNEK • M 051 323 343

[www.varen.it](http://www.varen.it)



ZAVAROVALNICA SAVA

# Popolna zaščita za mala in srednje velika podjetja

V POSLOVNEM SVETU, KJER SO TVEGANJA VSAKODNEVNA REALNOST, JE ZAŠČITA NEMOTENEGA POSLOVANJA KLJUČNEGA POMENA – ŠE POSEBEJ V OKOLJIH, KJER SO PODATKI, INFORMACIJSKI SISTEMI IN RAČUNALNIŠKA OPREMA OSNOVA ZA DELO.

Zato je podjetniško zavarovanje pametna naložba za vsakega sodobnega podjetnika.

## KAKO IZBRATI PRAVO ZAVAROVANJE?

Izbira pravega podjetniškega zavarovanja je ključnega pomena za varno in stabilno poslovanje. Pri tem je pomembno, da podjetje prepozna svoje potrebe – še posebej tveganja, povezana z uporabo informacijske tehnologije, digitalnimi storitvami, obdelavo podatkov in kibernetško varnostjo. Prav digitalna tveganja so danes med najpogostejšimi vzroki za motnje v poslovanju. Zato je pomembno, da znate sestaviti kombinacijo kritij, ki najbolje odgovarja dejanskim potrebam. Pri tem pa vam lahko seveda pomaga tudi izbrani zastopnik Zavarovalnice Sava.

## ZAKAJ IZBRATI PRENOVLJENI PAKET PODJETNIŠKIH ZAVAROVANJ?

Iz potrebe po individualni sestavi kritij so pri Zavarovalnici Sava prenovili Paket podjetniških za-

varovanj. Prenovljeno zavarovanje prinaša sodobno in individualno rešitev, ki je pisana na kožo malim in srednje velikim podjetjem ter samostojnim podjetnikom (s. p.). Kritija so zasnovana modularno, kar pomeni, da lahko sami izberete, katera kritija vključiti glede na naravo in obseg svojega poslovanja. Zavarovanje zajema tri ključne predmete, in sicer objekte (poslovne prostore), opremo (računalniki) in zaloge. Zavarovanju pa niso pozabili dodati novih kritij, ki omogočajo, da zavarovanje pokrije tudi širši spekter tveganj, kot sta npr. poškodovanje opreme ali naprav in kraja računalniške opreme.

Zavarovanje lahko oblikujete po meri, vključite dodatna kritija, ko jih potrebujete, in tako zavarujete tisto, kar je za vaše poslovanje resnično ključno.

Ker pa so obseg škode in posledično zneski za njeno sanacijo lahko hitro višji od pričakovanih, je pomembna tudi višina kritij. Novi paket omogoča visoke zavarovalne vsote, s katerimi boste v primeru škode ohranili finančno stabilnost in nadaljevali poslovanje brez večjih prekinitev. Ob sklenitvi permanentne police pa nudijo možnost ugodnejše premije.

## KOMU JE ZAVAROVANJE NAMENJENO?

Prenovljeno zavarovanje je oblikovano z mislijo na mala in srednje velika podjetja ter samostojne podjetnike (s.p.-je), predvsem pa je namenjeno podjetjem, ki želite poslovati varno, odgovorno in dolgoročno stabilno, tudi v nepredvidljivih okoliščinah. Je zanesljiv partner, ki poskrbi za celovito zaščito vašega podjetja. Zagotovite si brezplačno svetovanje na spletni strani Zavarovalnice Sava in preverite, ali je vaše podjetje ustrezno zavarovano.

Več najdete na spletni strani [www.zav-sava.si](http://www.zav-sava.si). (P.R.)

## Paket podjetniških zavarovanj



NIKOLI SAMI


**SAVA**  
ZAVAROVALNICA



TECH TRADE TRZIN

# Kakšno nadzorno kamero izbrati? Odvisno, za kaj jo potrebujete

KO KUPUJEMO NADZORNO KAMERO, POGOSTO ZAČNEMO NA NAPAČNEM KONCU.

Prebiranje tehničnih specifikacij, primerjanje ločljivosti in prečesavanje seznamov funkcij. To je napačen pristop k izbiri najprimernejše kamere. Najprej bi si morali zastaviti najpomembnejše vprašanje: kaj pravzaprav želimo s kamero opazovati.

## PONUDBA? NIKOLI VEČJA

V zadnjih letih je ponudba nadzornih kamer postala izjemno raznolika. Na voljo so kamere z baterijami, solarne kamere, kamere z internetno povezavo prek mobilnega omrežja, klasične Wi-Fi kamere za notranjo uporabo in profesionalni sistemi s kablji in snemalniki. Ker so razlike med njimi velike, je najbolj smiselno, da izbiro začnemo pri konkretnem scenariju uporabe.

## ALI SO OTROCI ŽE PRIŠLI DOMOV?

To je eden najbolj tipičnih scenarijev uporabe nadzornih kamer v stanovanju ali hiši. Starši želijo preveriti, ali so otroci prišli domov iz šole, ali so odprli vrata, ali se doma vse odvija normalno. V takšnem primeru običajno ne potrebujemo kompleksnega sistema z več kamerami, temveč preprosto notranjo IP kamero.

Takšna kamera je praviloma majhna, diskretna in se poveže z domačim brezžičnim omrežjem. Postavimo jo lahko na polico, omaro ali jo pritravimo na steno. S telefonom se nato povežemo v aplikacijo proizvajalca in lahko kadarkoli pogledamo sliko v živo.

Za takšen scenarij je zelo uporabna funkcija zaznavanja gibanja. Kamera ob zaznavi gibanja pošlje obvestilo na telefon, tako da uporabnik takoj vidi, da se je nekdo pojavil v prostoru. Še boljše je, če kamera uporablja prepoznavanje ljudi, saj tako razlikuje med človekom, hišnim ljubljencem ali zgolj premikajočo zaveso. Zelo praktična je tudi možnost dvosmerne komunikacije. To pomeni, da ima kamera mikrofoni in zvočnik, zato lahko starši prek aplikacije otrokom tudi kaj povedo. Kamere, ki vključujejo te tehnologije, lahko danes dobimo že za nekaj 10 evrov.

## KAKŠNO KAMERO POTREBUJEM ZA DOVOZ ALI VHOD PRED HIŠO?

Ko želimo nadzorovati dovoz ali vhod na dvorišče, se zahteve precej spremenijo. Kamera mora biti nameščena na prostem, delovati mora



v vseh vremenskih razmerah in imeti mora dober nočni način. Poleg tega mora imeti dovolj visoko ločljivost, da lahko jasno vidimo obraze ljudi ali registrske tablice vozil.

V takšnem primeru se zelo pogosto uporablja kamera, ki je povezana z omrežnim kablom. Takšne kamere uporabljajo tehnologijo PoE, kar pomeni, da po enem samem Ethernet kablju potujeta tako napajanje kot tudi podatkovni signal. Prednost takšne rešitve je predvsem zanesljivost. Kabelska povezava je bistveno stabilnejša od brezžične, poleg tega se ni treba ukvarjati z baterijami ali signalom Wi-Fi. Če ste prepričani, da je domači Wi-Fi signal dovolj močan, pa jo

lahko mirno povežete brezžično. Pri nadzoru dovoza je zelo koristna tudi kamera z vgrajeno lučjo. Ko kamera zazna gibanje, lahko samodejno prižge reflektor in osvetli območje pred hišo. To ima dvojni učinek. Najprej izboljša kakovost posnetka, saj kamera v temi vidi precej bolje, hkrati pa deluje tudi odvračilno. Močna svetloba pogosto že sama po sebi odvrne nepridiprave.

## KAKŠNO KAMERO POTREBUJEM ZA NADZOR CELOTNEGA DVORIŠČA?

Če želimo nadzorovati večji prostor okoli hiše, pogosto ni dovolj ena sama kamera. Hiše imajo več vhodov, različne strani dvorišča in pogosto tudi vrt ali garažo. V takšnih primerih se običajno uporablja kombinacija več kamer.

Na vhodu v hišo je pogosto nameščena kamera, ki pokriva vhodna vrata. Druga kamera spremlja dovoz, tretja zadnji del hiše ali vrt. Včasih se uporablja tudi kamera, ki se lahko obrača in nagiba. Takšne kamere omogočajo širši nadzor prostora, saj lahko z eno napravo pokrijemo precej večje območje.

Kamera, ki se lahko obrača in približuje sliko, je uporabna predvsem tam, kjer je prostor zelo velik. Kljub temu ima takšna rešitev tudi slabosti. Če kamera v določenem trenutku gleda v eno smer, lahko spregleda dogajanje na drugi strani. Zato se v praksi pogosto kombinira več fiksnih





kamer, ki stalno pokrivajo različne dele dvorišča. V primeru več kamer je dobro razmišljati vnaprej in kupiti izdelke istega proizvajalca. Tako lahko vse kamere najlažje spremljamo v isti aplikaciji in nam ni treba »skakati« iz ene v drugo.

#### POSEBNA REŠITEV JE KAMERA Z DVEMA LEČAMA

Danes so na voljo tudi zunanje kamere z dvojnimi sistemom leč, ki hkrati omogočajo širok pogled in nadzor nad okolico ter podrobnosti, ki jih želimo videti, ko gre kaj narobe. Ena širokokotna leča pokriva večje območje in skrbi za stalni pregled okolice, druga telefoto leča pa se lahko obrača ter zajame podrobnejše posnetke. Deluje pa tako: ko širokokotna kamera zazna gibanje, aktivira telefoto lečo, ki samodejno sledi osebi ali vozilu. Pri najboljših napredni algoritmi ločijo ljudi in avtomobile od drugih premikov, kar zmanjša število lažnih alarmov. Posnetke je mogoče shranjevati lokalno na kartico microSD, v oblak ali na omrežne naprave, povezava pa je možna prek kabla ali brezžično.

Takšna kamera je uporabna predvsem za nadzor zunanjih površin, kot so dvorišča, parkirišča, vhodi v hišo ali poslovne prostore. Zaradi kombinacije širokega pregleda in samodejnega sledenja lahko učinkovito pokrije večji prostor ter hitro zazna morebitne vsiljivce ali sumljivo dogajanje. Primerna je tako za domačo varnost kot tudi za manjša podjetja, skladišča ali počitniške



objekte, kjer je pomembno imeti pregled nad dogajanjem tudi na daljavo in v vseh vremenskih razmerah.

#### KAKŠNO KAMERO POTREBUJEM ZA VIKEND HIŠICO BREZ INTERNETA?

Veliko vikend hišic ima elektriko, nima pa stalne internetne povezave. V takšnem primeru klasične Wi-Fi kamere niso uporabne, saj potrebujejo internet za oddaljen dostop.

Ena izmed najbolj praktičnih rešitev je kamera z mobilno povezavo. Takšna kamera uporablja kartico SIM in se v internet poveže prek mobilnega omrežja in ne Wi-Fi omrežja ali kabla. Uporabnik lahko nato v aplikaciji na telefonu kadarkoli pogleda sliko v živo ali prejme obvestilo, če kamera zazna gibanje.

Takšne kamere so posebej priljubljene na oddaljenih lokacijah, saj pogosto vključujejo tudi baterijo ali celo solarni panel. To pomeni, da lahko delujejo tudi tam, kjer ni stalnega napajanja. Pri kamerah, ki jih napaja le baterija, je pomembno, da ne snemajo stalno, ampak se vklopijo le ob



zaznanem gibanju. Vmes pa baterijska kamera hrani energijo in zgolj čaka, da ji senzor sporoči, da se nekaj dogaja – takrat vklopi snemanje.

Druga možnost je kamera, ki sploh ne potrebuje interneta. Takšna kamera preprosto snema na pomnilniško kartico (ali ločen snemalnik, ki ga imate nekje v hiši). Posnetke si uporabnik pogleda kasneje, ko pride na lokacijo. To je preprosta in pogosto zelo poceni rešitev. Kompromis pa je, da v realnem času ne veste, kaj se na lokaciji dogaja.

#### RAD BI VIDEL LE, KDO ZVONI

Ne smemo pozabiti na video zvonce, ki postajajo vse pogostejši del sodobnih sistemov varovanja doma. Naprave združujejo funkcijo klasičnega zvonca in kamere, zato lahko uporabnik prek mobilne aplikacije takoj vidi, kdo stoji pred vrati. Ko nekdo pozvoni ali se približa vhodu, sistem pošlje obvestilo na telefon, uporabnik pa lahko obiskovalca vidi v živo, posname dogajanje ali z njim govori prek dvosmernega zvoka.



Takšna rešitev je uporabna za sprejem paketov, nadzor vhodnih vrat ali preverjanje dogajanja okoli hiše tudi takrat, ko nas ni doma.

#### KAKŠNO KAMERO POTREBUJEM NA JADRNICI ALI V AVTODOMU?

Na plovilih in v avtodomih so razmere nekoliko drugačne kot v hiši. Prostor je omejen, elektrika je pogosto na voljo le iz baterij, internet pa ni vedno zagotovljen.

Zato se v takšnih primerih pogosto uporabljajo kamere, ki imajo lastno baterijo. Te kamere snemajo predvsem takrat, ko zaznajo gibanje, zato lahko z enim polnjenjem delujejo precej dolgo – tudi mesec ali dlje. Če je na voljo mobilni signal, se lahko v internet povežejo prek mobilnega omrežja (s pomočjo kartice SIM).

Solarni panel lahko v takšnih primerih še dodatno podaljša avtonomijo delovanja, saj se kamera čez dan samodejno polni.

#### NAJPREJ SCENARIJ, ŠELE NATO KAMERA

Če pogledamo vse opisane primere, hitro postane jasno, da univerzalna kamera pravzaprav ne obstaja. Za nadzor doma je povsem dovolj notranja Wi-Fi kamera, medtem ko je za hišo z dvoriščem bolj smiselna kablenska PoE rešitev. Na oddaljenih lokacijah pa se največkrat izkažejo kamere z mobilno povezavo ali celo popolnoma samostojne baterijske naprave, morda celo s solarnim panelom.

Vse opisane rešitve najdete tudi na spletni strani [www.techtrade.si](http://www.techtrade.si). Če še vedno niste prepričani, so vam seveda na voljo za nasvete. Skupaj boste zagotovo našli pravo kamero za vaš scenarij. (P.R.)

**TECHTRADE**

[www.techtrade.si](http://www.techtrade.si)

**TECH TRADE d.o.o. Trzin**

Blatnica 8, 1236 Trzin

+386 1 562 21 11



## ESET MOBILE THREAT DEFENSE

# Zakaj bi direktor hotel zaščito mobilnih naprav?

**ESET MOBILE THREAT DEFENSE DIREKTORJEM OMOGOČA, DA Z INVESTICIJO V CELOVITO KIBERNETSKO VARNOST UČINKOVITO ZAŠČITJO TUDI MOBILNE NAPRAVE S POSLOVNIMI PODATKI IN KOMUNIKACIJO.**

S tem zagotovijo skladnost z zakonodajo in varnostnimi politikami – brez zapletov za zaposlene in IT.

SI-CERT je v svojih varnostnih poročilih izpostavil skokovit porast kibernet-skih varnostnih incidentov v povezavi z uporabo mobilnih naprav. Pri tem izstopajo lažna sporočila SMS – smishing, s povezavami do zlonamernih spletnih strani ter škodljiva programska oprema, ki krade bančne podatke, identitete (uporabniška imena in gesla) in druge vredne podatke v napravi. Grožnje mobilnim napravam prihajajo z vseh komunikacijskih kanalov, od SMS, Viberja, WhatsAppa, Facebook Messengerja in Instagrama, do aplikacij za skupinsko delo in deljenje datotek ter e-pošte in spleta. Zlonamerne-ži z mobilnimi napadi povzročajo vse večjo finančno škodo tako posameznikom kot podjetjem. Še posebej v podjetjih, kjer lahko zaposleni uporabljajo svoje mobilne naprave v službene namene, so varnostna tveganja toliko bolj pereča.

### KAJ JE PRI MOBILNI VARNOSTI SPLOH POMEMBNO?

Po podatkih, ki jih v ESET-u pridobivajo od uporabnikov, je za organizacije najbolj pomembna večplastna zaščita mobilnih naprav pred zlonamerno programsko opremo, phishingom in izsiljevalskimi napadi ter osrednje upravljanje. Z operativnega vidika si želijo učinkovitih funkcij, kot so oddaljeno zaklepanje, brisanje ali lociranje izgubljenih/ukradenih naprav ter nadzor nad aplikacijami in varnostnimi nastavitvami, recimo blokado neželenih aplikacij. Za potrebe skladnosti z zakonodajo pričakujejo tudi podporo za skladnost z varnostnimi politikami podjetja ter redno poročanje in opozarjanje na incidente.

ESET Mobile Threat Defense pri zaščiti naprav celovito naslavlja pričakovanja uporabnikov in z novimi zmožnostmi nenehno krepi kibernetško od-pornost organizacij.

**Večplastna zaščita:** napredni protivirusni pogon zaznava in blokira zlonamerno programsko opremo, napade z ribarjenjem ter izsiljevalsko program-sko opremo, kar zmanjšuje tveganje za okužbo naprav in krajo podatkov.

**Osrednje upravljanje:** vse mobilne naprave lahko upravljate, nadzorujete in konfigurirate iz ene spletne konzole – to omogoča hitro odzivanje na incidente in enostavno izvajanje varnostnih politik.

**Oddaljeno zaklepanje, brisanje ali lociranje:** če je naprava izgubljena ali ukradena, jo lahko na daljavo zaklenete, izbrišete podatke ali locirate, s čimer preprečite zlorabo poslovnih informacij.



*Pri poslovnih varnostnih rešitvah ESET PROTECT v paketih ADVANCED, COMPLETE, ENTERPRISE in ELITE ob vsaki licenci prejmete brezplačno licenco ESET Mobile Threat Defense za zaščito uporabnikove mobilne naprave.*

**Nadzor nad aplikacijami in varnostnimi nastavitvami:** določite, katere aplikacije so dovoljene, in nastavite varnostne politike, na primer obvezno geslo, šifriranje ... S tem zmanjšate tveganje uporabe nepooblaščenih ali nevarnih aplikacij.

**Redno poročanje in opozarjanje:** sistem samodejno pošilja poročila o stanju naprav in opozorila ob zaznanih incidentih, kar omogoča pravočasno ukrepanje.

**Podpora za skladnost:** ESET-ova mobilna zaščita pomaga zagotavljati skladnost z internimi in zakonskimi varnostnimi zahtevami ter standardi (ZVOP-2, ZInfV-1, ISO 27001, TISAX), saj omogoča nadzor nad obdelavo in zaščito osebnih in drugih kritičnih podatkov.

### JASNI VODSTVENI RAZLOGI ZA ESET MOBILE THREAT DEFENSE

Prvi razlog je zagotovo zaščita poslovnih podatkov. Mobilne naprave pogosto vsebujejo občutljive poslovne informacije, ESET PROTECT pa preprečuje izgubo ali krajo podatkov zaradi zlonamerne programske opreme ali napad smishing in phishing. Na drugi strani je nadzor. Osrednja upravljaljska konzola ESET Enterprise Inspector zagotavlja enostavno upravljanje in nadzor vseh naprav, tudi mobilnih, kar zmanjša tveganja in poenostavi varnostne IT-procese. Zakaj ne bi bili sodelavci za IT raje na voljo poslovnim uporabnikom za dvigovanje dodane vrednosti? Prenos kibernet-ske odpornosti še na mobilne naprave menedžerjem pod črto zagotavlja skladnost z zakonodajo, zmanjšanje tveganj vdora in odtokanja podatkov, izsiljevanja in drugih kibernet-skih groženj. Istočasno se ohranja produktivnost, saj zmanjšanje varnostnih incidentov neposredno zmanjša število motenj v poslovanju in prekinitev poslovnih procesov.

Več si lahko preberete na [www.sisplet.si](http://www.sisplet.si).

(P.R.)



DISTRIBUCIJA:  
**SI SPLET d.o.o.**  
Ukmarjeva 4, Ljubljana

01 428 94 05  
prodaja@sisplet.com  
[www.eset.com/si](http://www.eset.com/si)

ENGENIUS EXPERIENCE CENTER

# EnGenius – vrhunska omrežna tehnologija zdaj še bližje

ENGENIUS EXPERIENCE CENTER JE STIČIŠČE ZNANJA, INOVACIJ IN SODOBNIH OMREŽNIH REŠITEV, NAMENJENIH PODJETJEM, PARTNERJEM IN IT STROKOVNJAKOM, KI ŽELIJO IZBOLJŠATI SVOJO DIGITALNO INFRASTRUKTURO.

Podjetje Infnigate kot uradni distributer blagovne znamke EnGenius Networks v Sloveniji označuje odprtje novega EnGenius Experience Centra – prvega prostora pri nas, kjer lahko domači in poslovni uporabniki v živo preizkusijo najnaprednejše omrežne rešitve EnGenius.

EnGenius je globalni inovator na področju naprednih žičnih in brezžičnih omrežij, ki že več kot dve desetletji poganja povezanost za podjetja po vsem svetu.

## ZAKAJ ENGENIUS? OMREŽJA PRIHODNOSTI, DOSTOPNA DANES

EnGenius je sinonim za zanesljivost, varnost in preprostost upravljanja. Njihov portfelj vključuje:

- Najnaprednejše Wi-Fi sisteme, zasnovane za stabilno, hitro in varno povezavo – tudi v najbolj zahtevnih okoljih.
- Pametna stikala, ki optimizirajo podatkovni promet in zagotavljajo visoko stopnjo varnosti omrežja.
- Rešitve v oblaku – močno, fleksibilno in skalabilno upravljanje omrežij od kjerkoli, kadarkoli.
- Napredne tehnologije Wi-Fi 7, ki postavljajo nove standarde hitrosti in kapacitete (npr. nova AP-je serije ECW).
- AI-podprto upravljanje in varnost, ki preko EnGenius Cloud zagotavlja inteligentno optimizacijo in celovito vidljivost omrežja v realnem času.

Rešitve EnGenius so oblikovane za širok spekter industrij – od podjetij, hotelirstva in izobraževalnih ustanov do maloprodaje in večstanovanjskih objektov. Zasnovane so modularno in skalabilno, kar omogoča rast omrežja skupaj s potrebami uporabnikov.



## ENGENIUS EXPERIENCE CENTER – PROSTOR PREIZKUSA, ZNANJA IN INOVACIJ

Z novim Experience Centrom želijo EnGenius tehnologijo približati slovenskim podjetjem, integratorjem in IT strokovnjakom.

Obiskovalcem je na voljo praktično testno okolje, kjer lahko preizkusijo najnovejšo rešitve EnGenius Cloud, Wi-Fi 7 dostopne točke, stikala, AI-video nadzor in druge napredne tehnologije. V okviru centra potekajo tudi demonstracije realnih scenarijev, od podjetniških omrežij do naprednih rešitev za varovanje omrežij, obiskovalcem pa so na voljo strokovno svetovanje tehničnih specialistov in certificiranih trenerjev, ki pomagajo pri konfiguraciji, optimizaciji ter predstavitev novih funkcionalnosti. Na voljo je tudi možnost testnih implementacij, ki omogočajo preizkus delovanja naprav pred dejansko uvedbo v omrežje.



Experience Center je namenjen tako partnerjem kot končnim uporabnikom, ki želijo iz prve roke videti, kako lahko EnGenius poenostavi, pospeši in nadgradi njihovo digitalno infrastrukturo.

## ZANESLJIV PARTNER ZA DIGITALNO PRIHODNOST

Kot uradni distributer EnGenius v Sloveniji nudijo:

- strokovno podporo,
- hitro dobavo celotnega portfelja ter
- lokalne predstavitve in testna okolja.

EnGenius je zavezan k razvoju rešitev, ki so intuitivne, zmogljive in usmerjene v prihodnost - v podjetju Infnigate pa k temu, da te rešitve približajo slovenskemu trgu. (P.R.)

**infnigate**  
spark your growth

**Infnigate d.o.o.**

Ukmarjeva 4  
1000 Ljubljana

0590 14914  
info.si@infnigate.com

[www.infnigate.com/si](http://www.infnigate.com/si)



## DOMINO SISTEMI

# Celovita zaščita podatkov za mala in srednja podjetja

ZANESLJIVA IT PODPORA NI VEČ PRIVILEGIJ VELIKIH, POTREBUJEJO JO TUDI MALA PODJETJA, IN S PREMIŠLJENIMI REŠITVAMI LAHKO DOSEŽEJO VISOKO RAVEN VARNOSTI IN STABILNOSTI BREZ VELIKIH NOTRANJIH EKIP.

Mala podjetja pogosto nimajo dovolj virov, da bi vzpostavila in vzdrževala kompleksno IT infrastrukturo. Domino sistemi ponujajo prilagojene rešitve, ki združujejo varnost, zanesljivost in enostavno uporabo, ne glede na velikost podjetja.

### NADZOR IN VZDRŽEVANJE IT OPREME

Domino sistemi nudijo celoten spekter storitev: od nakupa in implementacije IT opreme do stalnega vzdrževanja, nadzora in optimizacije. Z rešitvijo Microsoft 365 omogočajo napredno delo v oblaku z integriranimi varnostnimi funkcionalnostmi, Microsoft Azure pa ponuja fleksibilno gostovanje aplikacij, razvojna okolja in povezavo z obstoječimi sistemi.

### VEČNIVOJSKA VARNOST

Domino sistemi implementirajo večnivojsko zaščito, ki zajema:

- **Končne naprave in strežnike** – zaščita pred zlonamerno programsko opremo, nepooblaščenim dostopom in ciljno usmerjenimi napadi.
- **Omrežje in požarne pregrade** – Stormshield zagotavlja zaščito kritične infrastrukture in skladnost z EU predpisi.
- **E-pošto in poslovne aplikacije** – nadzor, filtriranje in zaščita pred phishingom, nezaželeno pošto in ranljivostmi.

Celoten sistem temelji na dokumentirani varnostni politiki, kar omogoča jasen pregled, skladnost z notranjimi pravili in hitre odzive ob incidentih.

### BACKUP – ZANESLJIVA HRAMBA IN PRIPRAVA NA OBNOVITEV

Backup je ena ključnih komponent IT varnosti, ki pa je pogosto podcenjena. Domino sistemi zato



uvajajo celovito rešitev, ki združuje lokalno in oblako shranjevanje, avtomatizacijo ter redno preverjanje obnovljivosti podatkov.

Osnovo predstavlja večkopijski sistem, kjer so podatki shranjeni lokalno, v oblaki infrastrukturi in na oddaljenih lokacijah. Tak pristop omogoča hitro dostopnost ter visoko stopnjo redundance, saj so podatki v primeru izpada ali okvare še vedno na voljo drugje.

Pomemben element rešitve je tudi uporaba evropskega suverenega oblaka, ki zagotavlja varnost in skladnost z zakonodajo EU, vključno z GDPR. Podjetja imajo tako jasen nadzor nad lokacijo in lastništvom svojih podatkov.

Dodatno zaščito zagotavlja t. i. immutable backup, torej neizbrisne kopije podatkov, ki jih ni mogoče spreminjati ali izbrisati. Preprečuje zlonamerne spremembe, napade z izsiljevalskimi virusi in nenamerne napake uporabnikov, hkrati pa Immutable backup zagotavlja, da so vaše kritične datoteke vedno obnovljive, kar dodatno

povečuje odpornost podjetja. Rešitev vključuje tudi redne simulacije obnove in testiranja. Redno preverjanje integritete in obnove podatkov zagotavljajo, da so varnostne kopije (backupi) dejansko uporabne. Podjetja so tako pripravljena na morebitne incidente in prepričana, da postopki delujejo brezhibno.

Celovitost sistema dopolnjuje zaščita pred sodobnimi grožnjami, kot so izsiljevalski virusi, nepooblaščen dostopi ter napadi, pri čemer pomembno vlogo igrata šifriranje podatkov in nadzor dostopov. Za učinkovito ukrepanje pa poskrbijo tudi jasna dokumentacija in vnaprej določeni postopki, ki omogočajo hitro obnove podatkov, spremljanje stanja in beleženje incidentov, kar omogoča hitro odzivanje in skladnost z notranjimi varnostnimi politikami.

Tak sistem omogoča, da tudi mala podjetja z omejenimi IT viri vzpostavijo zanesljiv, skalabilen in varen backup, pripravljen na vsak incident ali izgubo podatkov.

### VARNOSTNI PREGLEDI IN STALNO SPREMLJANJE

Redni pregledi omrežja, končnih naprav in strežnikov omogočajo odkrivanje ranljivosti ter preprečevanje vdora ali izgube podatkov. Domino sistemi zagotavljajo stalni nadzor, posodobitev varnostnih politik in integracijo vseh varnostnih komponent. Več o njihovih rešitvah najdete na [www.domino-sistemi.si](http://www.domino-sistemi.si)

(P.R.)



**Domino sistemi d.o.o.**

Klementa Juga 7

5250 Solkan

Tel.: +386 5 33 33 670

Mob.: +386 41 632 055

[www.domino-sistemi.si](http://www.domino-sistemi.si)



# FREELIFE - PRILAGODLJIV SLOVENSKI CRM

## Brezplačen CRM po vaši meri

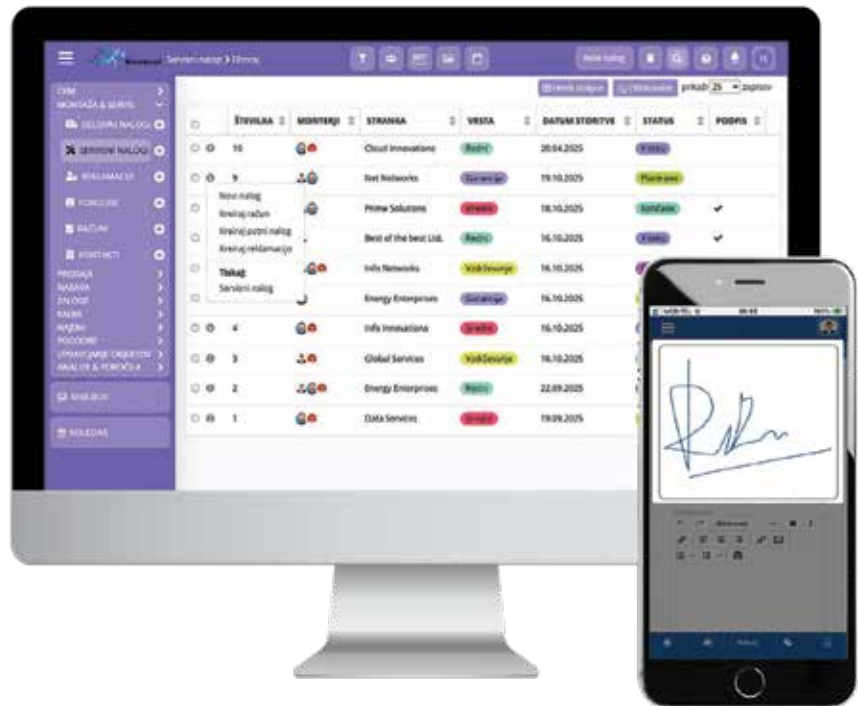
POSLOVNA PLATFORMA FreeLIFE PRINAŠA POPOLNO AVTOMATIZACIJO POSLOVANJA BREZ PROGRAMIRANJA. JE VEČ KOT CRM, SAJ ZDRUŽUJE PRODAJO, ZALOGE, KADROVANJE IN PROJEKTE.

Digitalizacija poslovanja postaja nujna, vendar se številna podjetja še vedno zanašajo na Excel preglednice in nabor različnih aplikacij. To pogosto pomeni **izgubo časa, slab pregled nad procesi in težje odločanje**. Prav na tem področju nastopa poslovna platforma FreeLife CRM. Rešitev, ki podjetjem **omogoča digitalizacijo in popolno prilagodljivost brez potrebe po programiranju**.

### KAJ PRINAŠA SISTEM IN ZAKAJ GA PODJETJA POTREBUJEJO?

Sistem FreeLife deluje po principu »no-code«, kar pomeni, da si lahko **podjetja svoje poslovne procese v celoti prilagodijo sama**. S tem se izognejo visokim stroškom programerskih storitev.

Aplikacija podjetjem prevzame breme vsakodnevnih administrativnih nalog, saj samodejno pošilja ponudbe, opomnike za neplačane račune in obvestila o novih povpraševanjih. Tako se zaposleni izognejo zamudnemu ročnemu vnašanju podatkov in se lahko osredotočijo na tisto, kar je resnično pomembno – na rast poslovanja. Platforma ne deluje le kot samo orodje za upravljanje s strankami, temveč **predstavlja celovito poslovno platformo**. Zdržuje vse ključne mo-



dule za uspešno vodenje podjetja: od izdajanja ponudb, delovnih nalogov, vodenja projektov, do upravljanja podatkov o zaposlenih in nadzora nad zalogami.

Rešitev je še posebej primerna za mala in srednja podjetja, ki želijo rasti, vendar jih omejujejo obstoječe aplikacije ali nepregledni procesi. Z uvedbo FreeLife rešitve lahko **podjetja izboljšajo učinkovitost, zmanjšajo napake in pridobijo boljši vpogled v svoje poslovanje**. Uporablja ga že več kot 300 podjetij v 6 državah. Za podjetja, ki še vedno uporabljajo Excel ali več nepovezanih orodij, je lahko to prvi korak k bolj strukturiranemu in učinkovitemu poslovanju.

Za hitro in brezhibno implementacijo skrbi mreža strokovnih partnerjev, ki nudi osebno podporo in svetovanje. Dober primer iz prakse je **podjetje Invoice d.o.o., ki dokazuje, da je mogoče sistem hitro in učinkovito prilagoditi** specifičnim potrebam najrazličnejših panog, od računovodstva do servisnih dejavnosti.

### ZAKAJ SE ZA DIGITALIZACIJO ODLOČITI ZDAJ?

Podjetja, ki želijo takojšen preskok v učinkovito digitalizirano poslovanje, se lahko na brezplačno uporabo prijavijo že danes na spletnih straneh **www.freelifecrm.com** ali **www.birokrat.si**. S tem korakom bodo znižala stroške in optimizirala svoje procese.

(P.R.)



### ZAKAJ FREELIFE?

- Ena aplikacija za vaše poslovanje (CRM, prodaja, delovni nalogi, projekti, zaloge, kadri)
- Manj ročnega dela in manj napak
- Avtomatizacija ključnih procesov
- Deluje na vseh mobilnih napravah
- Aplikacijo se vedno prilagodi vašim potrebam brez programiranja
- Povezljivost z računovodskimi in ERP sistemi
- Slovenska podpora in mreža partnerjev
- Uporablja ga že 300+ podjetij v 6 državah

### POPOLNA INTEGRACIJA IN STROKOVNA PODPORA

Ena največjih prednosti platforme FreeLife se skriva v **integraciji z računovodskimi sistemi in ERP programi, kot je Birokrat**. Podatki o dokumentih, partnerjih in računih se sinhronizirajo popolnoma avtomatsko in v realnem času, kar odpravlja vsakršno potrebo po ročnem izvozu ali uvozu podatkov. **Birokrat dodatno omogoča avtomatiziran zajem digitalnih dokumentov** ter izjemno enostavno elektronsko oddajo obrazcev na državne portale (FURS in AJPES).





ADVANT

# Bitka za podatkovne centre: priložnost, ki je Slovenija ne sme zamuditi

RAZCVET UMETNE INTELIGENCE IN DIGITALIZACIJE V ZADNIH LETIH MOČNO SPREMINJA EVROPSKI TRG PODATKOVNIH CENTROV.

O tem, kakšne priložnosti se odpirajo Sloveniji in kakšno vlogo imajo pri tem domača podjetja, smo se pogovarjali z Brankom Jovanovičem, tehničnim direktorjem za podatkovne centre v podjetju ADVANT.

## **Kako ocenjujete trenutno stanje na trgu podatkovnih centrov v Evropi?**

Evropski trg podatkovnih centrov doživlja izjemen razcvet. Pospešena digitalizacija in razvoj umetne inteligence sta povzročila, da povpraševanje po zmogljivostih že več let presega ponudbo, kar ustvarja pritisk na infrastrukturo in hkrati odpira nove priložnosti. Države, ki bodo znale pravočasno ukrepati, si lahko zagotovijo pomembno mesto na digitalnem zemljevidu prihodnosti – med njimi tudi Slovenija.

## **Ali lahko Slovenija postane regionalno digitalno središče?**

Evropa je že vstopila v fazo pospešenih zasebnih in javnih vlaganj v digitalno infrastrukturo, saj je obstoječa zmogljivost preprosto nezadostna. To ni trend, temveč strateški premik, v katerem se bo odločalo, kdo bo digitalno suveren in kdo odvisen. Slovenija ima redko priložnost, da se z odločnimi in hitrimi ukrepi postavi na zemljevid predvsem velikih zasebnih naložb v podatkovne centre. Če bomo ukrepali pravočasno in pritegnili te investicije v Slovenijo, bomo s tem močno okrepili IKT-ekosistem. To bo imelo velik vpliv tudi na celotno domače gospodarstvo. Če ne, bo ta razvojni val nepreklicno odšel drugam.

## **Kaj je še ključno za razvoj takšne infrastrukture v Sloveniji?**

Vzporedno z ukrepi na ravni države se morajo v Sloveniji krepiti tudi podjetja, ki se ukvarjajo z

načrtovanjem in gradnjo podatkovnih centrov. Če želi Slovenija postati regionalno digitalno središče, mora vzpostaviti močan domači ekosistem ponudnikov, ki bodo sposobni sodelovati tudi pri največjih in tehnološko najzahtevnejših projektih. Razvijati moramo lastne inženirske kapacitete, standardizirane procese ter sposobnost upravljanja kompleksnih projektov od zasnove do izvedbe. Takšna podjetja niso več zgolj klasična IT-podjetja. Poleg poznavanja informacijske tehnologije morajo obvladovati tudi ostala področja, pomembna pri izgradnji in obratovanju podatkovnih centrov.

## **Kako se je na te trende odzvalo podjetje ADVANT?**

Odločen korak v razvoju podjetja je bil narejen pred približno dvajsetimi leti, ko smo se strateško usmerili v področje podatkovnih centrov. Ta usmeritev ni bila naključna – temeljila je na razumevanju prihodnjih potreb trga. Podatkovne centre smo že zgodaj začeli obravnavati kot kompleksne sisteme kritične infrastrukture, kjer se prepletajo področja IT, energetike, hlajenja, fizikalnih zakonitosti delovanja infrastrukture, projektnega vodenja in zagotavljanja neprekinjenega delovanja. Takšen pristop zahteva razvoj specifičnih znanj in širokih kompetenc, hkrati pa omogoča gradnjo dolgoročnega zaupanja naročnikov.

## **Kako se projekti na tem področju spreminjajo?**

Sčasoma postajajo projekti vse zahtevnejši. Prehod z lokalnih rešitev na večje, energetske intenzivne sisteme je še posebej izrazit v zadnjih letih, ko razvoj umetne inteligence postavlja nove standarde glede zmogljivosti in energetske učinkovitosti. Prav na tem področju vidimo svojo pomembno konkurenčno prednost.

## **Kakšne priložnosti to odpira za slovenska podjetja?**

Ambicija Slovenije, da se pozicionira kot regionalno digitalno središče, pomeni tudi priložnost za podjetja, kot je ADVANT, da sodelujejo z velikimi mednarodnimi operaterji. Takšni projekti prinašajo višjo dodano vrednost, a tudi večjo kompleksnost.



Branko Jovanovič, tehnični direktor za podatkovne centre v podjetju ADVANT

## **Kakšni so vaši načrti za prihodnost?**

Naš cilj je postati pomemben tehnološki in razvojni partner pri gradnji digitalne Slovenije. Pri tem aktivno sodelujemo tudi v širšem ekosistemu in prispevamo k razvoju panoge. Leto 2026 bo predvsem obdobje utrjevanja kompetenc. Projekti postajajo vse večji in zahtevnejši, zato smo odprti tudi za povezovanja s strateškimi partnerji iz tujine, kar zna biti ključno za uspeh. Naš dolgoročni cilj ostaja jasen: postati prepoznaven regionalni strokovnjak za sodobno digitalno infrastrukturo.

## **Za konec – kako bi povzeli pomen razvoja podatkovnih centrov?**

Razvoj podatkovnih centrov ni več zgolj tehnološko vprašanje, temveč strateška priložnost – tako za podjetja kot za države. Slovenija ima vse pogoje, da jo izkoristi, odločilna pa bo pravočasna odločnost in jasno usmerjena vizija. (P.R.)



Advant d.o.o., Ljubljana,  
Cesta na Brdo 119A  
Telefon: +386 1 470 00 00  
E-pošta: info@advant.si  
www.advant.si

## CISO NA ZAHTEVO

# Potrebujete vodjo kibernetске varnosti, pa ga ne morete dobiti? Tu je rešitev

CISO NA ZAHTEVO JE MODEL, PRI KATEREM VLOGO VODJE INFORMACIJSKE VARNOSTI V DOLOČENEM OBSEGU PREVZAME ZUNANJI STROKOVNJAK.

Kibernetška varnost je v zadnjih letih iz tehnične teme prerasla v **eno ključnih odgovornosti vodstev podjetij**. Novi regulatorni okviri, kot so direktiva NIS2, ZInFV-1 in GDPR, od organizacij zahtevajo sistematičen pristop k upravljanju tveganj, odgovorno poročanje ter jasno določene vloge in odgovornosti.

V praksi to pomeni **imenovanje osebe ali funkcije, ki celovito pokriva področje kibernetске varnosti** – najpogosteje v obliki vloge CISO (Chief Information Security Officer).

### KAJ DANES POMENI VLOGA CISO

CISO ni več zgolj tehnični strokovnjak. Gre za vlogo, ki povezuje poslovne cilje, zakonodajne zahteve in obvladovanje tveganj. Njegove ključne naloge vključujejo:

- razvoj in nadzor izvajanja strategije informacijske varnosti,
- ocenjevanje in obvladovanje kibernetških tveganj,
- spremljanje skladnosti z zakonodajo in standardi,
- koordinacijo odziva na incidente ter poročanje vodstvu.

CISO deluje kot vezni člen med upravo, IT-jem, pravno službo in zunanjimi partnerji ter skrbi, da so varnostni ukrepi sorazmerni dejanskim tveganjem.

### IZZIV SLOVENSkih PODJETIJ: KADER, ČAS IN STROŠKI

Številne organizacije – zlasti mala in srednja podjetja ter javni subjekti – se pri tem soočajo z realnim problemom: **izkušenega CISO kadra je na trgu malo**, hkrati pa si ga pogosto ne morejo privoščiti kot redno zaposlitev.

Posledica so:

- razdrobljene odgovornosti,
- formalna skladnost brez prave vsebine,



- pomanjkljiva pripravljenost na incidente,
- in povečano osebno tveganje za vodstva.

### CISO NA ZAHTEVO KOT UVELJAVLJEN MODEL

Eden od odgovorov na ta izziv je model **CISO na zahtevo**, pri katerem podjetje v določenem obsegu vključi zunanjega strokovnjaka, ki prevzame vlogo vodje informacijske varnosti.

Takšen pristop omogoča:

- dostop do izkušenega strokovnega znanja brez zaposlovanja,
- neodvisen in objektivni pogled na varnostno stanje,
- podporo pri izpolnjevanju zahtev NIS2, ZInFV-1 in GDPR,
- strokovno podporo vodstvu pri varnostnih in investicijskih odločitvah.

### ZA KOGA JE TAK PRISTOP SMISELN?

Ta model se v praksi izkaže predvsem pri:

- organizacijah brez internega CISO kadra,
- podjetjih v procesu usklajevanja z NIS2 in ZInFV-1,
- vodstvih, ki želijo jasne in razumljive informacije o varnostnih tveganjih,
- ekipah, ki potrebujejo podporo pri presojah, incidentih ali uvajanju varnostnih ukrepov.

### KIBERNETSKA VARNOST KOT ODGOVORNOST VODSTVA

NIS2 in sorodna zakonodaja jasno sporočajo: kibernetška varnost ni več zgolj naloga IT-oddelka. Gre za **odgovornost uprave in vod-**

**stva** za ustrezno upravljanje kibernetске varnosti, kjer se od vodstev pričakuje aktivna vloga, razumevanje tveganj in sprejemanje utemeljenih odločitev.

Neustrezno upravljanje informacijske varnosti tako ni več zgolj operativno tveganje, temveč lahko pomeni tudi osebno odgovornost vodstvenih oseb, vključno z nadzornimi ukrepi ali sankcijami.

Vprašanje zato ni več, ali podjetje potrebuje CISO funkcijo – temveč **kako jo bo zagotovilo na učinkovit in vzdržen način.** (P.R.)



**CYBER  
SECURITY  
TEAM  
@ANNI**

**anni**  
www.anni.si

**Anni d.o.o.**

Motnica 7a, Trzin,

T: 01/ 5800 800 • info@varen.it

Toni JERŠIN • M 041 820 577

Matej PERNEK • M 051 323 343

**www.varen.it**



### SONIC RACING: CROSSWORLDS

Izid: 26. 3. 2026

Platforme: Nintendo Switch 2

Sonic Racing: CrossWorlds prinaša novo poglavje v seriji dirkalnih iger z modrim ježkom v glavni vlogi. Tokrat se poudarek premakne na raznolika okolja in dinamične proge, ki se med samo dirko spreminjajo in odpirajo nove poti. Znani liki iz sveta Sonica se vračajo z edinstvenimi vozili in sposobnostmi, ki vplivajo na potek dirk in omogočajo različne strategije.

Igra združuje arkadno hitrost z elementi tekmovalnosti, kjer so poleg vožnje ključni tudi pravočasni pospeški, uporaba predmetov in poznavanje prog. Poseben poudarek je na večigralskem načinu, ki spodbuja tako lokalno kot spletno tekmovalje.



### GREEDFALL: THE DYING WORLD – DELUXE EDITION

Izid: 31. 3. 2026

Platforme: PlayStation 5 in Xbox Series X|S  
GreedFall: The Dying World nadaljuje zgodbo prve igre z večjim poudarkom na političnih spletkah, raziskovanju in posledicah odločitev. Igralec se znajde v svetu, kjer starodavne sile in kolonialni interesi trčijo v boju za nadzor nad umirajočo deželo. V ospredju ostaja zgodba, podprta z razvejanimi dialogi in moralnimi odločitvami. Deluxe Edition poleg osnovne igre vključuje dodatne digitalne vsebine, kot so ekskluzivni oklepi, orožja in kozmetični dodatki, ki obogatijo začetno izkušnjo. Igra nadgrajuje sistem bojevanja z večjo taktično globino ter razširjenimi možnostmi razvoja lika.



### STARFIELD (STANDARD IN PREMIUM EDITION)

Izid: 7. 4. 2026

Platforme: PlayStation 5

Starfield je obsežna znanstvenofantastična RPG igra studia Bethesda Game Studios, ki igralce popelje v vesolje, polno raziskovanja, zgodb in svobode izbire. Dogajanje je postavljeno v daljno prihodnost, v kateri človeštvo raziskuje oddaljene zvezdne sisteme in išče odgovore na temeljna vprašanja o svojem obstoju. Igra omogoča ustvarjanje lastnega lika, raziskovanje planetov, upravljanje vesoljskih ladij ter sodelovanje v različnih frakcijah. Poseben poudarek je na svobodi igranja, saj igralec sam določa pot, ki jo bo ubral.

## Iskanje ključev je preteklost!



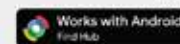
### XIAOMI Tag - pametni sledilnik

# 19,00€

**20% POPUSTA**  
OB NAKUPU 3 ALI VEČ



Deluje z:



Opozori na morebitno neželjeno sledenje in poskrbi za varnost zasebnosti.

10 g lahka zasnova z zaščito IP67 proti prahu in vodi



Xiaomi Store  
Europark Maribor

Xiaomi Store  
Supernova Rudnik

Xiaomi Store  
Citypark Ljubljana

[www.mi-store.si](http://www.mi-store.si)

## KUPUJETE ALI PRODAJATE RAČUNALNIŠKO OPREMO?

Oddajte svoj brezplačni oglas na [www.racunalske-novice.com/mali-oglas](http://www.racunalske-novice.com/mali-oglas)

### GoPro, Hero 7 Silver

Kamera deluje brezhibno in je bila testirana. Snema v 4K in ima touchscreen zaslon. Vidne so manjše sledi uporabe, ki ne vplivajo na delovanje. Priložen je tudi original



89,99 €

### Barvni laserski tiskalnik, Samsung

Prodajam multifunkcijski Samsung CLX-6260FW z napako. barvni tiskalnik, ločljivost tiskanja: do 9600 x 600 dpi, hitrost tiskanja: do 24 str/min (barvno), hitrost ...



250,00 €

### Polaroid Land Camera 1000

Prodajam vintage Polaroid Land Camera 1000 retro instant fotoaparata. Aparat je lepo ohranjen, normalen znak uporabe glede na starost, brez razpok ali poškodb ...



70,00 €

### HP 24 AIO PC All in One

AMD A8 7410, 8GB RAM, AMD Radeon R5, SSD 256GB, računalnik zmogljiv, kompakten in varčen vse v enem (AIO - All in One), vgrajen računalnik v 24" zaslonu. 200,00 €



### Asus Prime Z690-P Intel,

LGA1700, DDR5, ATX. Matična plošča je brez procesorja, diska in pomnilniških modulov. Originalna knjižica je priložena. Cena je zadnja.



100,00 €

### GeForce RTX 4060 Ti, 8 GB DDR6

Grafična je odlično ohranjena in še v garanciji, deluje brezhibno, nikoli uporabljena z overclockom, ni bila uporabljena za rudarjenje. Cena 400 Eur je zadnja.



400,00 €

### Segway, P65 Električni skiro

Praktično nov, odprta embalaža. Ni vožen / brez poškodb. Močan motor, doseg do 65 km. Trgovinska cena 900€+.



649,99 €

### Logitech, G29 Driving Force

(PS4/PS5/PC). Odlično ohranjen, volan in pedala delujejo brezhibno, brez tehničnih napak. Zelo lepo ohranjen, minimalni znaki uporabe, priložen ...



249,99 €

### Slušalke športne Philips TAA5508

Brezžične športne slušalke z odpravljanjem šumov. Malo uporabljene. Različni nastavitve za ušesa. Lahko pošljem po pošti.



60,00 €

### Samsung Galaxy A32 5G 64GB

Na prodaj je brezhiben in odlično ohranjen pametni telefon Samsung Galaxy A32 5G s 64 GB notranjega pomnilnika z etuijem in zaščitnim steklom...



50,00 €

### SSD SAMSUNG 860 PRO 256 GB SATA3

Prodajam nov zapakiran SSD, SAMSUNG 860 PRO 256 GB, 2,5", SATA3, V-NAND, MLC, 7 mm.



40,00 €

### Samsung s25 Ultra 512GB

Prodajam samsung s25 Ultra s 512GB spomina. Star je cca. 6 mesecev (v uporabi je bil samo slab mesec), in je dobro ohranjen. Nameščeno ima zaščitno steklo, ...



969,00 €

### HP EliteBook 840 G7 Intel Core i5

16GB RAM / 256GB SSD + DOCK. Prenosnik se ponaša z zmogljivim in varčnim štirijedrnim procesorjem Intel Core i5-10210U, ki deluje pri osnovni frekvenci 1,6 GHz ...



249,00 €

### INTEL procesor za prenosni računalnik

- I80/2M/800  
- LF80537 T7100  
- FRU 42W7654  
- SLA4A  
- Odlično ohranjen in delujoč, ...



15,00 €

### Slušalke Razer Kraken Quartz

Prodajam gaming slušalke Razer Kraken Quartz. Slušalke so zelo lepo ohranjene in delujejo brezhibno. Lahko se prevzame v Kranju ali Ljubljani.



49,99 €

### 16 GB DDR4 RAM 3200mhz

Za prenosnik Micron SODIMM (kit 2x 8GB) 3200mhz. Modula sta popolnoma delujoča in brez napak. Primerna za večino prenosnikov in mini računalnikov ...



55,00 €

### Napajalnik Dell

685W 80+ Gold H685EF-00 za strežnike/delovne postaje. Brezhiben napajalnik Dell 685W 80+ Gold H685EF-00, primeren za strežnike/delovne postaje, ...



50,00 €

### ASUS grafična kartica

Dual Radeon RX 580 0 8GB. Prodajam ASUS grafična kartica Dual Radeon RX 580 0 8GB. Imam več komadov (8 kom.). Če kupiš vse dam količinski popust.



100,00 €

### Asus K55VJ Intel i7, 8GB RAM,

USB mikrofoni z zelo dobrim studijskim zvokom, primeren za streaming, gaming, podcast ali ustvarjanje vsebin. Deluje brezhibno, priložen je original kabel ...



119,99 €

### Napajalnik ATX Excelvan 850W

Prodajam brezhiben ATX napajalnik znamke Excelvan nazivne moči 850W ter maksimalne moči do 1050W. Zmožen pogonjati sisteme z večimi, ...



45,00 €

### Thermalright Burst Assassin 120 ARGB

Prodajam nov zapakiran CPU hladilnik + dodaten ARGB ventilator. Za podnožja: Intel: 115X/1200/1700/1851, AMD: AM4/AM5. Priložim še 1 dodatni nov Thermalright ...



25,00 €

### Lenovo Ideapad Slim 5 15Iru9 i5-120U

16gb RAM/512gb SSD/WIN 11/ Garancija. Prodajam eleganten in zmogljiv prenosnik, odličen za delo, šolo ali zabavo. Zelo hiter in tih prenosnik, primeren za ...



575,00 €

### Gaming računalnik i7

16 GB RAM / GTX 1070 / 756GB SSD / 4TB HDD. Prodajam na novo sestavljen in popolnoma očiščen gaming računalnik. Sveža namestitve Windows 10 Pro (aktivirani) ...



229,00 €

### AMD Ryzen 7 1700 – 8 jeder, 16 niti

AMD Ryzen 7 1700 (3.0-3.7 GHz, 8 jeder / 16 niti) z originalnim Wraith Spire hladilnikom, ki ga priložim zraven. Procesor deluje brezhibno, nikoli ...



45,00 €

### Macbook Pro 16' – Apple M1 Pro

Z naprednim procesorjem Apple M1 Pro 10-core, ki deluje pri 2,1 GHz in doseže turbo frekvenco do 3,2 GHz, opremljen s 32 GB RAM-a in 1 TB SSD diskom ...



1.799,00 €

### Instax mini 11 – instant fotoaparata

Kamera je lepo ohranjena, malo uporabljena in deluje brezhibno. Uporablja Instax Mini film. Ima samodejno prilagajanje osvetlitve, selfie način in vgrajeno bliskavico.



60,00 €

### Xiaomi 15 Ultra, 512 GB, 16 GB RAM

Prodajam vrhunsko ohranjen telefon (6,73-palčni) jasen zaslon z ločljivostjo 3200 x 1440 pik, AMOLED WQHD+, frekvenca osveževanja 120 Hz, 68 bilijonov barv, HDR10+ ...



940,00 €

### 3D tiskalnik Artillery Genius Pro

Na prodaj 3D tiskalnik Artillery Genius Pro, odličen za vse, ki iščejo kakovostno in zanesljivo rešitev za 3D tiskanje. Ta model je nadgrajen z PEI magnetno ploščo ...



80,00 €

### Prodajam grafično kartico MSI GTX 970

GAMING 4G GEFORCE GTX 970. Proizvajalec: MSI (OC gaming serija). Grafični procesor: NVIDIA GeForce GTX 970. Vmesnik: PCI Express 3.0 x16.



50,00 €

### TAMRON SP 150-600 F/5-6,3 Di VC USD G2

Na prodaj je odličen objektiv, ki je v izjemno dobrem stanju. Ta objektiv je bil zelo malo rabljen, kar pomeni, da je še vedno v odlični ...



800,00 €

### Prodajam Philips LED monitor

18 palčni Philips LED monitor 197E, ki ga odlikujeta odlična kakovost slike in eleganten izgled. Ločljivost 1366 x 768, TFT zaslonska plošča, format, ...



40,00 €

### Lenovo ThinkPad L470

Prodajam brezhibno delujoč, tovarniško obnovljen (Refurbished), laptop Lenovo ThinkPad L470. Samo resni, prosim. Procesor Intel Core i5-7200U, RAM 8GB, ...



90,00 €

### AirPods 4

Prodajam brezžične slušalke Apple AirPods 4, ki so nove in še originalno zapakirane. Te vrhunske slušalke blagovne znamke Apple prinašajo izjemno kakovost zvoka in ...



120,00 €

### Napajalnik ATX Excelvan 850W

Prodajam brezhiben ATX napajalnik znamke Excelvan nazivne moči 850W ter maksimalne moči do 1050W. Zmožen pogonjati sisteme z večimi ...



45,00 €

### Nokia N97 - 4 Mini RM-555

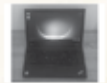
Redek model, odklujen na vse sim kartice, priložen originalni polnilec.



90,00 €

### Lenovo Thinkpad L570 i5 7200u

8GB RAM, SSD nov, zaslon 15.6" Anti-Glare, procesor Intel Core i5-7200u 2.7GHz Turbo do 3.1GHz, integrirana grafična Intel HD Graphics 620, nadgrajen SS, ...



170,00 €

### Gaming PC Microstar intel i5,

8GB RAM, Nvidia GTX 1050 Ti 4GB, SSD, prodajam Gaming PC Microstar (MSI) sestavljen iz sledečih komponent: Osnovna plošča: MSI MS-7728 H61



160,00 €

### ASUS PRIME Z370-P Motherboard

INTEL Matična plošča, idealna za vse, ki iščejo zanesljivo in zmogljivo osnovno ploščo za Intel procesorje. S formatom ATX omogoča



Po dogovoru

### Monitor Dell UltraSharp 43" 4k IPS

Monitor Dell UltraSharp 43" 4K IPS - idealen za poslovno in pisarniško uporabo. Ta impresiven 43-palčni zaslon ponuja izjemno ločljivost 3840x2160 (4K) ...



380,00 €

Objavljeni oglasi so bili aktualni ob prijavi revije.

Za ogled najnovejših ponudb skeniraj QR kodo.





# Kako pirati zlomijo zaščito Netflixa in ostalih?



DIGITALNA DOBA JE PRINESLA UDOBJE, O KATEREM SMO NEKOČ LAHKO LE SANJALI. CELOTNE KNJIŽNICE FILMOV IN SERIJ SO NA VOLJO Z ENIM KLIKOM.

Toda v ozadju poteka boj med multimilijardnimi korporacijami (Netflix, Disney+ ...), ki so oborožene z najsodobnejšimi algoritmi za šifriranje, in piratskimi skupinami, ki iščejo načine, kako se dokopati do brezplačnih vsebin.

Ko se na piratskih spletnih straneh pojavi nova serija, ki je izšla le pred nekaj urami, se človek lahko samo vpraša, kako piratom uspe čisto vsakič preliščiti filmske gigante. So celo bolj uspešni kot piratske skupine, ki pripravljajo »cracke« za igre.

## KAJ SPLOH JE DRM?

Da bi razumeli, kako pirati zlomijo zaščito, moramo najprej razumeti, kaj sploh napadajo. Ključna kratica je DRM (Digital Rights Management) oziroma digitalno upravljanje pravic. Lahko bi rekli, da gre za ključavnico, vendar je to preveč splošno. V bistvu je to celoten ekosistem protokolov, ki določajo, kdo, kje in na kakšen način lahko gleda določeno vsebino.

Najbolj razširjen med njimi je Googlov Widevine, ki ga uporablja večina pretočnih platform (Netflix, Disney+, HBO Max). Poleg njega poznamo še Applov FairPlay in Microsoftov PlayReady. Ti sistemi delujejo na principu šifriranja video datoteke, ki jo vaš brskalnik ali pametna naprava odklene le, če ima veljaven digitalni ključ.

## L1, L2, L3 ... KAJ POMENIJO TE OZNAKE?

Widevine L3 je najšibkejša stopnja zaščite. Dešifriranje poteka povsem na programski ravni (v brskalniku). Ker ključi potujejo skozi sistemski pomnilnik, jih je relativno enostavno prestreči. Posledica? Netflix na napravah z zaščito L3 omeji ločljivost na 480p ali največ 720p.

Widevine L1 je sveti gral DRM zaščite. Dešifriranje poteka v izoliranem, varnem okolju procesorja (angl. TEE – Trusted Execution Environment). Ključi nikoli ne zapustijo strojne opreme v berljivi obliki. To omogoča predvajanje v ločljivosti 4K s podporo HDR.

Pirati se ne trudijo z zlomom samega algoritma AES-128 (Advanced Encryption Standard (128-bit) – to je eden najbolj razširjenih algoritmov za šifriranje podatkov na svetu.) To bi s trenutno računalniško močjo trajalo tisočletja. Namesto tega iščejo poti okoli njega.

## NAPAD NA SAMO SRCE STROJNE OPREME

Najnovejša razkritja v varnostnih krogih, predvsem raziskave, kot je projekt Wideshears, so pokazala, da niti stopnja L1 ni neprebojna. Medtem ko so starejše metode temeljile na prestrezanju ključev v programski opremi (L3), Wideshears cilja neposredno na okolje Qualcomm Trusted Execution Environment (QTEE).

Wideshears uporablja ranljivosti v t.i. Trusted Applications (TA), ki tečejo znotraj procesorja. Heckerji so ugotovili, da lahko prek specifičnih ukazov v pomnilniku izzovejo puščanje informacij.



Postopek vključuje iskanje ranljivosti v TA, kar pomeni, da morajo identificirati napake v kodi, ki upravlja s ključi znotraj varnega območja procesorja. V nadaljevanju morajo izvleči t. i. korenjski ključ oziroma Keybox, ki je unikaten za vsako napravo. Z njegovo pomočjo lahko pirati na svojem računalniku poustvarijo celoten dešifrirni proces. Na koncu ostane še ekstrakcija iz SFS (angl. Secure File Storage). S pomočjo Wideshears so raziskovalci in tudi pirati uspeli pridobiti podatke iz območja varnega shranjevanja, kjer se hranijo najbolj varovani certifikati.

To pomeni, da pirati ne potrebujejo več fizičnega dostopa do zaslona za »snemanje«, temveč lahko z uporabo teh ukradenih strojnih ključev neposredno prenesejo originalno, neokrnjeno 4K datoteko.

## KDO IMA VEČ STRELIVA?

Večina sodobnih piratskih objav z oznako WEB-DL temelji na uporabi ukradenih ključev CDM (angl. Content Decryption Module). Piratske skupine (EVO, NTG ali novejša anonimne celice) uporabljajo ranljivosti v specifičnih Android napravah za t. i. CDM dumping, kar vključuje izkoriščanje varnostnih lukenj v jedru operacijskega sistema, da bi iz procesorja izvlekli dešifrirne ključe.

Ko piratska skupina enkrat pridobi veljaven ključ Widevine L1, lahko njihova programska oprema prepriča Netflixove strežnike, da je njihov računalnik dejansko certificiran pametni televizor ali vrhunski pametni telefon. Strežnik nato pošlje video v najvišji možni kakovosti (4K, Dolby Vision), ki ga pirati s pomočjo ukradenega ključa preprosto shranijo v nešifrirani obliki.

Netflix in Google nista nemočna. Ko opazita, da se določen certifikat uporablja za masovno piratstvo, ga prekličeta, zato je piratstvo filmov in serij, predvsem v ločljivosti 4K, postalo vprašanje ekonomije in zalog. Vsak ukraden CDM ključ (certifikat), ki omogoča dostop do 4K vsebine, ima svojo življenjsko dobo. Takoj ko piratska skupina objavi film v 4K, Netflixovi varnostni sistemi zaznajo uporabo tega certifikata in ga v nekaj dneh (včasih urah) uvrstijo na črno listo.

Zato piratske skupine pogosto hranijo svoje najboljše L1 ključe za velike premiere (novo sezono Stranger Things ali House of the Dragon). Manj pomembne serije raje objavijo le v različici ločljivosti 1080p, ki uporablja manj dragocene L3 ključe, ki jih je lažje nadomestiti. Temu pravijo »varčevanje s strelivom«.

Ko zmagajo Netflix in ostali, so piratske skupine primorane objaviti datoteko z oznako WEB-Rip. V tem primeru morajo uporabiti zmogljive zjemalne kartice (angl. capture cards), ki prestrežejo video signal, ko ta zapusti napravo prek HDMI kabla. Čeprav so te naprave opremljene z zaščito HDCP (angl. High-bandwidth Digital Content Protection), obstajajo razdelilniki, ki to zaščito odstranijo. Slika se nato ponovno zakodira, kar povzroči le minimalno izgubo kakovosti, a v očeh piratskih puristov WEB-Rip nikoli ne doseže statusa WEB-DL.

### ALI PIRATI URE IN URE BEDIJO PRED ZASLONI?

Seveda ne. Predstavljajte si, da bi posamezniki morali ročno dekodirati čisto vsako serijo ali film, ki se pojavi na pretočnih platformah. Nemogoče. Namesto tega uporabljajo skripte, ki proces v veliki meri avtomatizirajo.

Skripta sproži prijavo v Netflix z uporabo veljavnega (ukradenega ali kupljenega) računa. Samo dejno pridobi metapodatke, izbere vsebino, preveri vse razpoložljive jezike podnapisov in zvočnih zapisov. Ko je čas za avtorizacijo licence, skripta iz baze uporabi veljaven CDM ključ. Potem sledi prenos šifriranih delčkov videa, ki jih v realnem času dešifrira in sestavi v končno datoteko (običajno v formatu .mkv). Takoj, ko je datoteka pripravljena, se samodejno naloži na zasebne strežnike (angl. seedbox), od koder se s pomočjo torrentov razširi na javne in zasebne strani.

Koliko časa traja celoten postopek? Pet minut ali manj za 45-minutno epizodo serije.

### ZAKAJ NETFLIX NE USPE ZATRETI ODPORA PIRATOV?

Morda se zdi nenavadno, da podjetja z milijardnimi proračuni ne morejo ustaviti skupine hakerjev. Razlog tiči v sami naravi digitalne distribucije. Da bi uporabnik vsebino lahko videl, jo mora njegova naprava dešifrirati. In kjer koli se vsebina dešifrira, obstaja teoretična možnost, da

se ta postopek prestreže. Poleg tega Netflix bije bitko na tisočih frontah. Podpirati mora vse od najnovejših iPhoneov do deset let starih pametnih televizorjev in poceni Android TV škatel iz Kitajske. Vsaka od teh naprav je potencialna šibka točka. Če Netflix popolnoma zapre dostop vsem napravam, razen tistim z najstrožjo zaščito, bo izgubil na milijone naročnikov, ki imajo starejšo opremo. Pirati to razpoko med varnostjo in dostopnostjo s pridom izkoriščajo.

### TUDI UMETNA INTELIGENCA JE V POMOČ PIRATOM

V redkih primerih, ko piratskim skupinam ne uspe prelisčiti pretočnih velikanov in jim izpred oči izmakniti filme in serije v ločljivosti 4K, še vedno obstaja možnost »upscalinga«. Kot smo že omenili, 1080p vsebino je mnogokrat lažje prestreči kot 4K. V tem primeru se lahko uporabi UI modele za umetno povečanje ločljivosti na 4K, hkrati pa se odstrani še šum in izboljša ostrino. Rezultati so včasih tako dobri, da povprečen uporabnik ne loči razlike med originalnim 4K prenosom in UI izboljšanim posnetkom.

### GLOBOKO V PIKSLIH SE SKRIVAJO VODNI ŽIGI

Ker tehnološka zaščita pogosto odpove, se Netflix in drugi zatekajo k forenzičnemu označevanju. Gre za nevidne digitalne podpise, vgrajene v video signal. Ti znaki so edinstveni za vsakega naročnika ali regijo.

Če se na spletu pojavi piratska kopija, lahko Netflixovi inženirji analizirajo datoteko in ugotovijo, iz katerega računa je bila vsebina ukradena. Vendar so pirati razvili protiukrepe – algoritme, ki primerjajo več različnih posnetkov iste vsebine in odstranijo elemente, ki niso skupni vsem (torej vodne žige).

### IMA TA VOJNA LAHKO KONČNEGA ZMAGOVALCA?

Bitka za dešifriranje Netflixja je klasičen primer tehnološke tekme v oboroževanju. Vsakič, ko korporacije zgradijo višji zid, pirati uporabijo daljšo lestev ali pa zgradijo tunel pod zemljo. Čeprav so DRM sistemi, kot je Widevine L1, izjemno napredni, popolna varnost ne obstaja. V tej vojni po vsej verjetnosti ne bo končnega zmagovalca. Pred desetletjem, čisto na začetku industrije pretočnosti, se je govorilo, da so pirati blizu izumrtja. Ne zato, ker niso uspeli zlomiti zaščite, ampak zato, ker je bila legalna ponudba dobra in dostopna. Od takrat pa so vsi ponudniki pretočnih vsebin redno višali cene, kčili ponudbo, jo fragmentirali in podobno. Ideja, da moraš biti prijavljen na tri ali več tovrstnih platform, ni več tako privlačna (in poceni), kot je bila nekoč. In to je voda na mlin za piratstvo, ki je spet v porastu.


AKTUALNO

## ODDAJA NA RADIU, PRISLUHnite NAM!

Na vašem najljubšem radiu prisluhnite tedenskim oddajam, ki jih za vas pripravljamo v uredništvu Računalniških novic.

<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I ZELEN VAL</div> <p style="font-size: 8px;">93,1 MHz 96,2 MHz 97,0 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiozelenvall.com</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I KRKA</div> <p style="font-size: 8px;">106,6 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiokrka.com</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I Univox</div> <p style="font-size: 8px;">99,5 MHz 106,8 MHz 107,5 MHz</p> <p style="font-size: 8px; text-align: center;">www.univox.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I ALFA</div> <p style="font-size: 8px;">103,2 MHz 107,8 MHz</p> <p style="font-size: 8px; text-align: center;">www.radio-alfa.si</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I moj radio</div> <p style="font-size: 8px;">107 MHz 102,6 MHz</p> <p style="font-size: 8px; text-align: center;">www.mojradio.com</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I KRANJ</div> <p style="font-size: 8px;">97,3 MHz</p> <p style="font-size: 8px; text-align: center;">www.radio-kranj.si</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I ROBIN</div> <p style="font-size: 8px;">99,5 MHz 100 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiorobin.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I NOVA</div> <p style="font-size: 8px;">106,9 MHz</p> <p style="font-size: 8px; text-align: center;">www.radionova.si</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I ODMEV</div> <p style="font-size: 8px;">90,9 MHz 97,2 MHz 99,5 MHz 103,7 MHz</p> <p style="font-size: 8px; text-align: center;">www.radio-odmev.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I ŠTAJERSKI VAL</div> <p style="font-size: 8px;">93,7 MHz 87,6 MHz</p> <p style="font-size: 8px; text-align: center;">www.radio-stajerski-val.si</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I GEOSS</div> <p style="font-size: 8px;">89,7 MHz</p> <p style="font-size: 8px; text-align: center;">radiogeoss.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I Velenje</div> <p style="font-size: 8px;">107,8 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiovelenje.com</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I OGNJIŠČE</div> <p style="font-size: 8px;">104,5 MHz 105,9 MHz 107,3 MHz</p> <p style="font-size: 8px; text-align: center;">radio.ognisisce.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I SORA</div> <p style="font-size: 8px;">89,8 MHz 91,1 MHz 96,3 MHz</p> <p style="font-size: 8px; text-align: center;">www.radio-sora.si</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I NTR</div> <p style="font-size: 8px;">91,1 MHz 107,1 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiotomi.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I 94</div> <p style="font-size: 8px;">98,2 MHz 97,8 MHz 104,1 MHz 102,6 MHz 100,2 MHz</p> <p style="font-size: 8px; text-align: center;">www.radio94.si</p>
<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I TOMI</div> <p style="font-size: 8px;">94,6 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiotomi.si</p>	<div style="background-color: #2e8b57; color: white; padding: 2px; font-weight: bold; text-align: center;">RADIO I SRAKA</div> <p style="font-size: 8px;">94,6 MHz</p> <p style="font-size: 8px; text-align: center;">www.radiosraka.com</p>



					AVTOR: BOTY	HERCEGOVSKO MESTO OB MERETVI	VSAKOLETNI PIVSKI PRAZNIK V MUNCHNU	NAŠA NEKDANJA SMUČARKA (MATEJA)	SLADKO-VODNA RIBA, KAPELJ	ANGLEŠKA IGRALKA IN PEVKA (JILL)	LUKA V ITALIJSKI APULIJI
1	2	3	4	5	TROPSKI KOMAR						
					DEFEKT, NAPAKA						
					NAPRAVA ZA AEROBNO VADBO			2			
					KRALJ VZHODNIH GOTOV						
					TERME V V. BELGIJI						
<b>:DRUŽINSKI ZABAVNIK</b>	MAVČNA OPORNICA	NAPAD NA POLITIČNO OSEBO	OBLIKA IMENA IGNAC	JEZERO V KAMBODŽI PEVEC *MO-DRIJANOV* (BLAZ)				ZEN NA KITAJSKEM NEKO. NAS SM. SKAK. (PETER)			
GRASČINA NA DOLENSKEM									NIKOLA TESLA ITALIJSKA ROCKERKA (GIANNA)		
TRAVA DRUGE KOŠNJE							KROŽNO KRZIŠČE ALBANSKI DRŽAVNIK (RAMIZ)				
NAŠA PEVKA FALK					@	ZAHODNO-SKOTSKI OTOK				Z IKONAMI OKRAŠENA STENA	RASTLINA TROPSKE AMERIKE
GIULIO NATTA			BALETNI PLESALEC								
			KOŽNO VNETJE, SEN								
PLESNA FIGURA PRI ČETVORKI				ANIMIRANI FILM							3
				TEKSTIL							
SOL ALI ESTER VINSKE KISLINE								ATOM Z ELEKTR. NABOJEM AM. REŽISER ASTER			
GRŠKI POLOTOK Z ATENAMI					REKA NA JUGU ŠKOTSKE	AMERIŠKA FILMSKA IGRALKA KENDRICK					
<b>:DRUŽINSKI ZABAVNIK</b>	ŽIVOT, POSTAVA	AMERIŠKI IGRALEC (BILLY)	INDIJSKA ZAČIMBA				KIINI MODEL VOZILA				REZERVOAR ZA GORIVO
				4			PETELINJI BOJ				
OBRITO-GLAVEC					SMUČI				STANLEY TUCCI		
					VODNA ŽIVAL S KLESCAMI				SL. PEVEC SMOLAR		
SAMICA TAPIRJA								OČE			
								OLIVER TWIST			
PULJSKA ZNAMENITOST						NAŠA SMUČARSKA SKAKALKA (NIKA)					1
ZELO MOČEN ČLOVEK						MOČAN PRIJEM Z ROKAMI					

## Križanke in uganke za vse okuse



Informacije in naročila

**Bogat denarni nagradni sklad:**  
**3.500 €**  
**Prva nagrada:**  
**1.500 €**



### NAGRADE in NAGRAJENCI

Med reševalce, ki bodo do petka, **10. 4. 2026.** poslali pravilno rešitev, bomo z žrebom razdelili privlačne nagrade:

**3x miška White Shark AZRAEL Black**



V žrebu sodelujete tako, da pošljete rešitev križanke (oštevilčeni kvadrati) s svojimi podatki (ime in priimek, naslov, pošta številka in pošta) na elektronski naslov [narocnine@stromboli.si](mailto:narocnine@stromboli.si). Rešitev brez kontaktnih podatkov ne bomo upoštevali pri žrebu.

Bluetooth slušalke SBOX EB-TWS99 prejemejo:

- Irena Krnc, Ljubljana
- Peter Bizjak, Grosuplje
- Monika Rauh, Ljubljana

Nagrade podarja podjetje Stromboli, d.o.o.

Rešitev križanke 4/XXXI: EKLAN



**KOLEDAR DOGODKOV**

ERIZIPEL: šen, TOTILA: kralj Vzh. Gotov, SAB: jezero v Kambodži, TARANTO: luka v Italiji, ESK: reka na jugu Škotske

## KOLOFON



**Izdajatelj:**  
 Stromboli, marketing, d. o. o.  
 Cesta komandanta Staneta 4A,  
 1215 Medvode

**Glavni in odgovorni urednik:**  
 Boštjan Štrukelj,  
 tel.: 01 / 620 88 01

**Vsebinski urednik:**  
 Niko Bajec,  
 tel.: 01 / 620 88 05  
[niko.bajec@stromboli.si](mailto:niko.bajec@stromboli.si)

**Narocnine:**  
 tel.: 01 / 620 88 00,  
[narocnine@stromboli.si](mailto:narocnine@stromboli.si)

**Oglasno trženje:**  
 Matej Komprej, tel.: 01 / 620 88 06  
 gsm: 070 / 606 152, [matej.komprej@stromboli.si](mailto:matej.komprej@stromboli.si)

Boštjan Štrukelj, tel.: 01 / 620 88 01,  
 gsm: 041 / 663 301, [boštjan.strukelj@stromboli.si](mailto:boštjan.strukelj@stromboli.si)

Ana Kopitar, tel.: 01 / 620 88 09,  
[ana.kopitar@stromboli.si](mailto:ana.kopitar@stromboli.si)

**Sodelavci in novinarji:**  
 Maja Lavrač, Matej Saksida, Peter Čebren  
 Blaž Ulaga, Jana Breznik, Jan Sladič,  
 Matej Komprej, Boštjan Štrukelj,  
 Niko Bajec in Tanja Pirnat

**Fotografije:** Arhiv Računalniške novice

**Tisk:** Tiskano v Sloveniji

**Distribucija:**  
 EKDIS d. o. o., Stromboli, marketing, d. o. o.

**Oblikovanje in DTP:**  
 Tanja Pirnat s.p., [dtp@stromboli.si](mailto:dtp@stromboli.si)

**http://www.racunalniske-novice.com**  
 Računalniške novice (Online)  
 ISSN 1581-047X

Na podlagi zakona o davku na dodano vrednost spada revija med proizvode, za katere se obračunava DDV po stopnji 5 %.  
 ISSN 1408-4872

Nenaročenih rokopisov in fotografij ne vračamo. Pisem bralcev in oglasov ne lektoriramo.

Vse gradivo v reviji Računalniške novice je last izdajatelja. Kopiranje ali razmnoževanje je možno le s privoljenjem izdajatelja. Poštnina za naročnike plačana pri pošti 1102 Ljubljana. Revija Računalniške novice je vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo RS, pod zaporedno številko 661.

Predstavitve, ki jih objavljamo v reviji in so označene z rubriko Predstavitve in na koncu članka s (P.R.) – Payable Release (plačani članek) – pripravljamo v sodelovanju s podjetji.

Sporočila za javnost sprejemamo na [Rn@stromboli.si](mailto:Rn@stromboli.si). Izid revije je finančno podprla Javna agencija za raziskovalno dejavnost Republike Slovenije.

2026

# WEBSI

Digitalni presežki slovenije

Prijave so odprte!

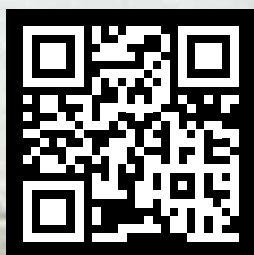
Zgodnje prijave do 21. aprila



BAG.SI

# KOLESARSKÉ TORBE ZA VSAK OKUS.

Tvoj slog. Tvoja pot.



IZBERI SVOJO NA  
[WWW.BAG.SI](http://WWW.BAG.SI)