Računalniške novice

Cena: 1,99 €

V Evropi še eno leto brezplačne zaščite za Windows 10

št. 13-14/XXXI
9. julij 2026

KIBERNETSKA VARNOST JE POSTALA PREIZKUS ODPORNOSTI

Odprtokodna orodja, ki lahko zamenjajo znane in drage rešitve

Huawei Watch Fit 5 Pro: ura, ki je prerasla športno zapestnico

Obveščevalne službe opozarjajo na nevarnost umetne inteligence

Poceni spletni nakupi izven EU so postali dražji

Ste si v Whatsappu že rezervirali svoje uporabniško ime?

Android 17 bo končno bolje izkoristil zložljive zaslone

Zmogljiv in zanesljiv

HP priporoča Windows 11 Pro za podjetja.

9H7U6ET

HP ProDesk 4 Tower G1i

Zagotovite si povračilo denarja za nove naprave HP z operacijskim sistemom Windows 11, medtem ko zamenjate svoje stare računalnike katere koli znamke z HP Trade-In.

HP ProDesk 4 v G1i ohišju stolpa rastočim podjetjem zagotavlja ključne funkcije za storilnost v cenovno ugodnem namiznem računalniku z umetno inteligenco. Zmogljiv in zanesljiv z izbiro grafičnih kartic, procesorjem Intel® Core™ Ultra in nevronsko procesorsko enoto z zmogljivostjo 13 bilijonov operacij na sekundo, ki z razdeljevanjem moči in raziskovanjem potenciala umetne inteligence za izboljšanje poslovne učinkovitosti pomaga optimizirati vsakodnevne naloge.

Operacijski sistem

Windows 11 Pro

Procesor

Intel® Core™ Ultra 5 225 (do 4,9 GHz, 10 jeder, 10 niti)

Pomnilnik

16-GB pomnilnik DDR5-5600 MT/s

Notranji pomnilnik

512-GB pogon SSD PCIe® NVMe™ M.2

Že za 1.598,20 EUR

Za več informacij in naročilo obiščite
www.src.si/hp-windows-11-pro

* Program je namenjen izključno HPjevim komercialnim partnerjem. Vračilo velja za zamenjavo ene stare naprave za eno novo napravo HP z operacijskim sistemom Windows 11. HP bo preveril posredovane informacije in si pridržuje pravico do preverjanja originalnega dokazila o nakupu in dokazila o odstranitvi starih naprav iz lasti končnega uporabnika. Povačilo partnerju bo izplačano do konca julija 2026. HP si pridržuje pravico zahtevati vračilo v primeru neupoštevanja določil in pogojev programa. HP si pridržuje pravico, da kadar koli spremeni pogoje promocije brez predhodnega obvestila ali prekine promocijo. HP ne odgovarja za tehnične ali uredniške napake. Ponudba velja do 31.7.2026 ali do odprodaje zalog in je na voljo izključno pri pooblaščenih distributerjih.

Microsoft znova podražil konzole Xbox Series X in Series S

Microsoft je napovedal novo občutno podražitev konzol Xbox Series X in Xbox Series S. Nove cene bodo začele veljati 1. avgusta 2026, razlog pa je, na presenečenje nikogar, pomanjkanje pomnilnika in shrambe.

Podražitev bo tokrat precejšnja. Modeli s 512 GB prostora bodo dražji za 100 ameriških dolarjev, modeli z 1 TB prostora pa za približno 150 dolarjev. Microsoft bo hkrati umaknil iz prodaje 2 TB različico Xbox Series X Galaxy Black, ki je bila doslej najdražji model v ponudbi. Tudi evropske cene bodo dvignili za enako vrednost.

To pomeni, da bo Xbox Series S s 512 GB prostora po novem stal približno 499 €, medtem ko je prej stal okoli 399 €. Xbox Series S z 1 TB prostora se bo s približno 449 € podražil na približno 599 €. Xbox Series X Digital, torej različica brez optičnega pogona, bo namesto okoli 599 € stala približno 749 €. Klasični Xbox Series X z optičnim pogonom pa se bo s 649 € podražil na približno 799 €. Najdražji Xbox Series X Galaxy Black, ki je stal okoli 699 €, kot rečeno umikajo iz ponudbe.

Microsoft pojasnjuje, da se je v zadnjih mesecih trudil najti rešitev z dobavitelji, vendar so se cene pomnilnika in shrambe močno zvišale. To ni prva podražitev Xbox konzol. Microsoft je cene zvišal že maja 2025, nato v ZDA še enkrat oktobra 2025. Nova podražitev je še toliko bolj neprijetna, ker cene višajo v obdobju, ko bi morale konzole trenutne generacije po običajni logiki postajati dostopnejše. Xbox Series X in Series S sta na trgu že od leta 2020, kar pomeni, da smo globoko v življenjskem ciklu generacije. Namesto popustov in cenejših paketov pa kupci plačujejo več.

Najbolj nenavaden je položaj Xbox Series S. Ta je bil ob izidu zamišljen kot cenovno najdostopnejša vstopnica v novo generacijo konzol. Bil je manj zmogljiv od Series X, brez optičnega pogona, z manj prostora in zato bistveno cenejši. Z novo ceno približno 499 € za model s 512 GB pa ta argument ni več tako prepričljiv. Konzola je še vedno najcenejši Xbox, vendar je precej manj dostopna, kot je bila na začetku.

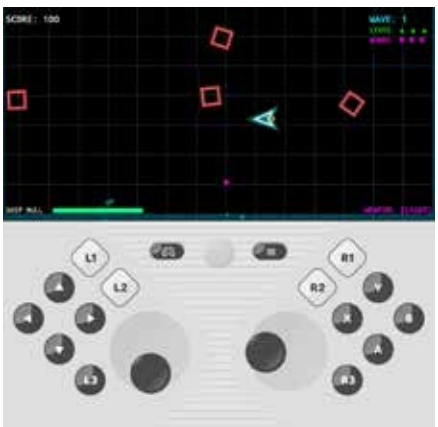
Ob takšnih podražitvah se seveda pojavi zelo neprijetno vprašanje, zakaj bi kupec sploh izbral Xbox, če je PlayStation 5 zmogljivejši, ima boljše igre in je cenejši? Xbox sicer ima Game Pass, odlično združljivost s starejšimi igrami, pogosto zelo dobro integracijo z osebnim računalnikom in oblačnim igranjem, pod svojim okriljem pa ima tudi nekaj zelo močnih studiev. A to so močni argumenti le za uporabnika, ki je že v Microsoftovem svetu ali mu veliko pomeni naročniški dostop do iger. Za povprečnega kupca, ki danes izbira novo konzolo, pa je računica vse težja. Če mora za Xbox Series X plačati več kot za PS5, hkrati pa dobi strojno manj prepričljivo in tržno manj dominantno platformo, bi moral Microsoft ponuditi zelo jasen razlog, zakaj ostati pri Xboxu.

Android 17 bo končno bolje izkoristil zložljive zaslone

Android 17 bo dobil namenski igralni način za zložljive telefone, ki bo izkoristil eno največjih prednosti takšnih naprav: velik zaslon. Nova funkcija bo polovico zaslona spremenila v navidezni igralni plošček s tipkami na dotik, druga polovica pa bo ostala namenjena sami igri. V bistvu gre za funkcijo, ki jo že nekaj časa podpirajo emulatorji, zdaj pa bo privzeto na voljo v celotnem sistemu.

Ideja je preprosta, a obenem zelo smiselna. Zložljivi telefoni imajo dovolj velik zaslon, da lahko ob odprti napravi del prostora namenijo upravljanju, ne da bi s tem povsem uničili igralno izkušnjo. Pri običajnih telefonih navidezne tipke pogosto prekrijejo del dogajanja v igri, pri zložljivih napravah pa lahko Android kontrole prestavi na ločeno polovico zaslona. Tako igralec dobi občutek, ki je bližje ročni igralni konzoli.

Novi način, ki naj bi bil na voljo v prihodnjih mesecih, bo deloval kot sistemski navidezni igralni plošček. Po pojasnilih strokovnjaka za Android Mishala Rahmana bo krmilnik na sistemski ravni posnemal pritiske fizičnih tipk, zato naj bi deloval z vsako igro, ki podpira fizične igralne kontrolerje. Navidezni igralni plošček bo vključeval skoraj vse, kar pričakujemo od sodobnega kontrolerja. Na voljo bodo smerni križec, leva in desna analogna palica, tipke A, B, X in Y, ramenske tipke L1, L2 in L3, desne tipke R1, R2 in R3 ter tipka Start. Google bo omogočil tudi nekaj prilagajanja. Uporabnik bo lahko nastavil, ali sta navidezni analogni palici poravnani ali zamaknjeni, prilagodil bo lahko velikost tipk ter vklopil ali izklopil haptične povratne informacije.



Vklop funkcije naj bi bil zelo enostaven. Rahman pravi, da bo dovolj, da uporabnik razpre zložljivo napravo pred zagonom združljive igre ali po njem. Android bo nato ponudil oziroma omogočil igralni način.

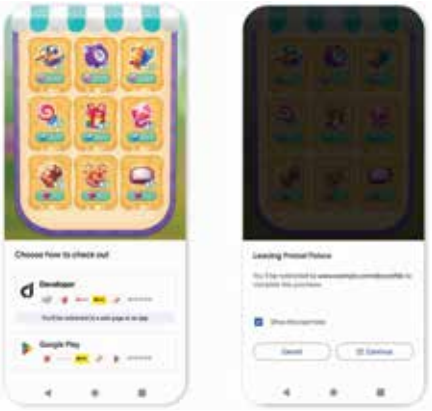
Uporaba namenskega krmilnika bo še vedno boljša izbira, vendar bo za tiste, ki ga nimajo, to dobra alternativa.

Play Store bo omogočal tudi zunanja plačila

Google bo po letih pritiskov, tožb in regulatornih postopkov končno bolj odprl trgovino Google Play za zunanje načine plačevanja. Sprememba pomeni, da razvijalci aplikacij za Android ne bodo več nujno vezani samo na Googlov plačilni sistem, uporabniki pa bi lahko pri nekaterih aplikacijah plačevali neposredno razvijalcem ali prek alternativnih plačilnih rešitev.

Google Play je bil dolgo zgrajen okoli modela, pri katerem Google razvijalcem zagotovi distribucijo aplikacij, plačilni sistem in infrastrukturo, v zameno pa od nakupov v aplikacijah in naročnin pobere provizijo. Najbolj znana je bila 30-odstotna provizija, ki je postala simbol spora med velikimi tehnološkimi platformami in razvijalci. Zdaj se ta model spreminja. Google napoveduje, da bo enotno 30-odstotno nadomestilo zamenjal z nižjimi in bolj ločenimi provizijami. To pomeni, da bo Google delno ločil plačilo za uporabo trgovine od plačila za uporabo Googlovega plačilnega sistema. Če bo razvijalec uporabil alternativno plačilno rešitev ali bo uporabnika preusmeril na svojo spletno stran, bo struktura provizij drugačna, kot če bo uporabil Google Play Billing.

Kolikšen delež bo Google vzel od posamezne transakcije, ne bo več odvisno samo od ene pavšalne stopnje. Pomembno bo, ali gre za uporabnika, ki je aplikacijo prvič namestil pred uvedbo novega sistema ali po njej, koliko razvijalec letno zasluži in ali uporablja Googlov plačilni sistem. Če bo razvijalec še vedno uporabljal



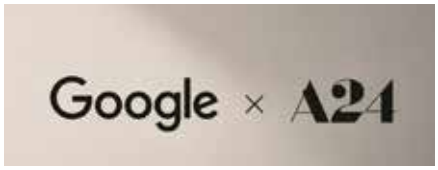
Google Play Billing, bo Google zaračunal dodatnih 5 % nadomestila za plačilni del.

Za aplikacije, ki letno ustvarijo več kot milijon dolarjev prihodkov, naj bi osnovne stopnje znašale 20 % za nove nakupe v aplikacijah in 10 % za naročnine. To je še vedno precejšen delež, vendar je nižji od dolgo kritizirane 30-% provizije. Hkrati pa Google s tem jasno sporoča, da popolnoma brezplačne distribucije prek storitve Play Store ne bo. Tudi če razvijalec uporabi svoj način plačila, Google še vedno zaračuna dostop do platforme, trgovine, varnostnega sistema, distribucije in uporabniške baze.

Spremembe so povezane s protimonopolno tožbo Epica proti Googlu. Čeprav sodišče še ni dokončno potrdilo obsežne poravnave, s katero bi rešili spor glede Googlovega domnevnega monopola nad distribucijo aplikacij za Android, Google torej že začenja uvajati spremembe v pravilih za razvijalce.

Za uporabnike bo sprememba lahko pomenila več izbire. Pri nekaterih aplikacijah se bodo lahko pojavili gumbi za plačilo zunaj Googlovega sistema, povezave na spletne strani razvijalcev ali alternativni načini nakupa naročnin. V idealnem primeru bi to lahko pomenilo nižje cene, saj razvijalec ob nižji proviziji del prihranka prenese na uporabnika. V praksi pa ni nujno, da se bo to zgodilo. Google želi spremembe usmerjati tako, da ne izgubi popolnega nadzora nad kakovostjo aplikacij. Podjetje uvaja tudi programe, kot sta Games Level Up in Apps Experience, ki naj bi nagrajevali kakovostne aplikacije in igre z nižjimi stopnjami. Za vključitev v te programe bodo morale aplikacije izpolnjevati določene pogoje, kot so delovanje na več vrstah naprav (na primer tablicah, pametnih televizorjih ali Android Auto), dobre vrednosti pri porabi pomnilnika in pri stabilnosti ter podpora priporočenim funkcijam, kot so shranjevanje v oblaku ali varnejši načini prijave. Uvajanje sprememb ne bo povsod enako hitro. Nekatere spremembe bodo v določenih regijah začele veljati že konec septembra, druge do konca leta, globalna uvedba pa naj bi se nadaljevala po 30. septembru 2027.

Google in A24 razvijata nova filmska orodja z umetno inteligenco



Google DeepMind in neodvisni filmski studio A24 sta sklenila večletno raziskovalno partnerstvo, s katerim želita razvijati nova orodja za filmsko produkcijo. Po poročanju The Wall Street Journala naj bi Google v A24 vložil približno 75 milijonov ameriških dolarjev, kar je tudi prvi primer, da je Google pridobil lastniški delež v filmskem studiu. Uradno sporočilo govori o sodelovanju med enim najmočnejših raziskovalnih laboratorijev za umetno inteligenco in studiem, ki slovi po avtorskem pristopu k filmu. Cilj naj bi bil razviti nove delovne tokove in tehnike, ki bi ustvarjalcem pomagale razširiti možnosti pripovedovanja zgodb. Google poudarja, da želi orodja prihodnosti oblikovati skupaj z ljudmi, ki jih bodo dejansko uporabljali.

Za zdaj ni znano, pri katerih filmih ali projektih bo Google sodeloval. Partnerstvo naj bi se razvijalo skozi več projektov, osredotočeno pa bo na povezovanje napredne tehnologije in zabavne industrije. Po poročanju The Wall Street Journala dogovor ni ekskluziven, kar pomeni, da lahko A24 sodeluje tudi z drugimi partnerji. Pomembna podrobnost je tudi, da Google ne bo dobil dostopa do filmske in televizijske knjižnice studia A24. Kljub temu bo sodelovanje verjetno sprožilo precej razprav. Za filmsko industrijo je umetna inteligenca zelo občutljiva tema, predvsem zaradi vprašanj avtorskih pravic, uporabe podatkov za učenje modelov in strahu, da bi tehnologija zmanjšala vlogo ustvarjalcev. Več velikih studiev je zaradi domnevnih kršitev avtorskih pravic že zelo ostro nastopilo proti podjetjem, ki razvijajo umetno inteligenco.

A24 in Google naj bi v razvoj vključila tudi nekatere ustvarjalce iz kroga studia A24. Med njimi se omenja Kane Parsons, režiser filma Backrooms, ki je v preteklosti javno kritiziral generativno umetno inteligenco. Prav zato bo zanimivo spremljati, ali bodo nova orodja res služila ustvarjalcem ali pa bodo v Hollywoodu sprejeta kot še en poskus tehnoloških podjetij, da vstopijo v filmsko produkcijo.

Partner neodvisnega filmskega studia A24 Scott Belsky pravi, da orodja ne bodo podobna klasičnim generatorjem vsebin na ukaz. Po njegovih besedah obstajajo boljši načini uporabe umetne inteligence, ki ohranjajo ustvarjalni nadzor in obenem omogočajo več eksperimentiranja.

V Evropi še eno leto brezplačne zaščite za Windows 10

Po novem se bo obdobje kritičnih varnostnih popravkov za operacijski sistem Windows 10 namesto oktobra 2026 izteklo šele 14. oktobra 2027. Microsoft je spremembo vpeljal precej ne-

opazno, saj jo je na svojo uradno podporno stran dodal zgolj kot popravek za program Windows 10 ESU.

S tem so uporabniki, ki ne morejo ali preprosto nočejo preiti na Windows 11, dobili dodatnih 12 mesecev časa, v katerem bodo tudi z uporabo Windowsa 10 lahko varno uporabljali svoje računalnike. Pri Microsoftu poudarjajo, da gre za njihovo zavezo k varnosti uporabnikov med tranzicijo, ki jim bo dala več časa in omogočala več prilagodljivosti za iskanje primerne nove strojne opreme.

Za evropske uporabnike je situacija še posebej ugodna. Zaradi preteklih pritiskov organizacij za varstvo potrošnikov se lahko posamezniki v Evropi v program prijavijo popolnoma brezplačno. Tu namreč zadošča že zgolj prijava z Microsoftovim računom. Drugod po svetu morajo uporabniki za brezplačen dostop sinhronizirati nastavitve preko orodja Windows Backup ali unovčiti 1.000 Microsoftovih nagradnih točk, sicer pa je na voljo tudi enkratno plačilo v znesku približno 27 evrov. Posamezna licenca ESU sicer pokriva do 10 naprav, povezanih z istim računom. Velja pa opozoriti, da je ta program strogo omejen na osebne računalnike. Naprave, ki so del poslovnih domen ali podjetniškega upravljanja, do teh brezplačnih popravkov niso upravičene. Čeprav Windows 11 trenutno obvladuje približno 73 odstotkov trga namiznih računalnikov, ostaja na 26 odstotkih teh naprav še vedno trdno zasidran Windows 10. Glavni razlog za to so stroge strojne zahteve novejšega sistema, kot sta modul TPM 2.0 in Secure Boot. Zaradi tega okoli 400 milijonov aktivnih računalnikov po svetu uradno sploh ne izpolnjuje pogojev za nadgradnjo. Situacijo za te uporabnike dodatno zapleta kriza na trgu komponent. Zaradi izjemnega razcveta umetne inteligence namreč prihaja do pomanjkanja pomnilniških čipov, saj proizvajalci, kot so Samsung, SK Hynix in Micron, zmogljivosti usmerjajo v napredne AI pospeševalnike. Posledično so se pogodbene cene pomnilnikov DRAM od začetka lanskega leta praktično podvojile, analitiki pa napovedujejo ponovno podražitev. Cene računalnikov, tablic in telefonov naj bi se do konca leta 2026 dvignile za 10 do 20 odstotkov. Nakup novega računalnika je torej trenutno izjemno draga poteza. Za tiste, ki kljub temu ne želijo ostati na nezaščitenem sistemu, sicer ostajajo na voljo nekatere alternativne rešitve, kot so neuradni popravki podjetja 0patch do leta 2030 ali migracija na operacijski sistem Linux.

Obveščevalne službe opozarjajo na nevarnost umetne inteligence

Najtesneje povezana obveščevalna zavezništva na svetu – ZDA, Združeno kraljestvo, Kanada, Avstralija in Nova Zelandija – opozarjajo, da bi lahko bili najnaprednejši modeli umetne inteligence že kmalu sposobni izvajati kibernetske napade, ki bodo presegli zmogljivosti današnjih obrambnih sistemov. V skupni izjavi je zavezništvo Five Eyes vlade in podjetja pozvalo, naj z ukrepi ne odlašajo. Po njihovem mnenju ne gre več za vprašanje prihodnosti, temveč za neposredno varnostno tveganje.

Najostrejši del opozorila predstavlja ocena časovnice. Po navedbah obveščevalnih služb razvoj naprednih UI modelov poteka hitreje, kot je pričakovala industrija. Modeli naj bi kmalu bistveno spremenili tako napadalne kot obrambne zmogljivosti na področju kibernetske varnosti. Umetna inteligenca ni več zgolj tehnološka inovacija, temveč vprašanje nacionalne varnosti. To je prvič, da tako jasno opozorilo prihaja iz najvišjih varnostnih institucij.

Opozorilo je sledilo kmalu po odločitvi ameriške administracije, da omeji uporabo najzmogljivejših modelov podjetja Anthropic za tuje državljane. Razlog je bil model Mythos 5, ki je pokazal izjemne sposobnosti pri odkrivanju varnostnih ranljivosti. Pri Anthropicu so kasneje pojasnili, da so ameriške oblasti odkrile način, kako bi bilo mogoče obiti zaščitne mehanizme javnega modela Fable 5. Zaradi tega podjetje in ameriška

vlada že več tednov sodelujeta pri iskanju ustreznih rešitev.

Posledica vsega tega je, da se največje UI laboratorije vse pogosteje obravnava podobno kot podjetja, ki razvijajo kritično infrastrukturo. Po mnenju strokovnjakov največje nevarnosti ne grozijo največjim korporacijam. Velika podjetja praviloma že vlagajo v napredne sisteme kibernetske zaščite in imajo specializirane varnostne ekipe. Veliko bolj izpostavljena so mala in srednje velika podjetja, ki pogosto nimajo zadostnih sredstev za sodobno zaščito. Strokovnjaki opozarjajo, da bi prav ta podjetja lahko postala prve žrtve prihodnje generacije UI napadov.

Obveščevalne službe pa poudarjajo tudi zanimiv paradoks. Ista tehnologija, ki omogoča napadalcem hitrejše iskanje ranljivosti, lahko pomaga tudi obrambnim ekipam.

Umetna inteligenca že danes omogoča hitrejše odkrivanje varnostnih lukenj, analizo nenavadnega vedenja v omrežjih, avtomatsko preverjanje programske kode in hitrejše odzivanje na incidente. Vprašanje zato ni, ali moramo UI uporabljati v kibernetski varnosti, ampak kdo jo bo znal uporabljati čim bolj učinkovito.

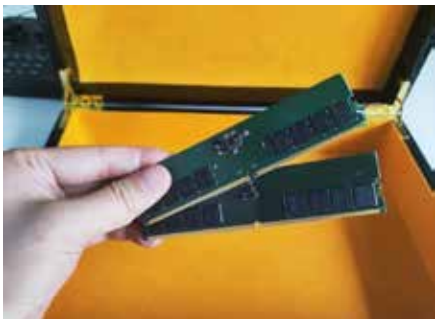
Hiter razvoj seveda odpira tudi politična vprašanja. V ZDA še vedno ne obstaja enoten sistem za ocenjevanje tveganj najzmogljivejših UI modelov. Del strokovnjakov poziva k strožji regulaciji, drugi pa opozarjajo, da bi lahko prevelike omejitve upočasnile inovacije.

Zato vse več raziskovalcev predlaga bolj odprt in transparenten sistem preverjanja varnosti modelov, kjer bi sodelovali tako razvijalci kot neodvisni varnostni strokovnjaki.

Opozorilo zavezništva Five Eyes kaže, da se razprava o umetni inteligenci iz tehnoloških konferenc vse bolj seli v varnostne institucije.

Če so bile doslej glavne teme produktivnost, avtomatizacija in delovna mesta, se zdaj v ospredje postavlja vprašanje, kako zaščititi države, podjetja in kritično infrastrukturo pred sistemi, ki bodo morda že kmalu sposobni izvajati zelo napredne kibernetske napade.

So cene sistemskega pomnilnika dvigovali namerno?



Trije največji svetovni proizvajalci pomnilniških čipov, družbe Samsung, SK hynix in Micron, so se znašli sredi odmevnega pravnega spora. Skupinska tožba, vložena na zveznem sodišču v Kaliforniji pod imenom Garciaguirre proti Samsung Electronics, skupino obtožuje nezakonitega usklajevanja z namenom umetnega omejevanja zalog in dvigovanja cen. Omenjena trojica skupaj obvladuje približno 90 odstotkov celotnega svetovnega trga sistemskih pomnilnikov, kar jim daje ogromno moč.

Pri tem velja omeniti, da sta Samsung in SK hynix v preteklosti že priznala krivdo v kazenskem postopku zaradi dogovarjanja cen sistemskega pomnilnika. Podjetje SK hynix pa je aprila 2005 že plačalo kazen v višini 185 milijonov dolarjev. Najnovejša obtožnica navaja, da so podjetja izkoristila prehod na visokoprepustni pomnilnik (HBM) – napredno tehnologijo, ki se uporablja za pospeševalnike umetne inteligence. To naj bi storila z namenom, da prikrijejo namerno zmanjšanje proizvodnje starejših in standardnih modulov DDR3 ter DDR4. Ker postavitev nove tovarne za proizvodnjo pomnilnikov stane na desetine milijard evrov in zahteva več let dela, na trg ni mogel vstopiti noben nov tekmec, ki bi zapolnil nastalo vrzel. Posledično so cene poskočile do rekordnih vrednosti, kar so na svoji koži občutili tudi končni potrošniki. Med 17 tožniki je 14 posameznikov in tri majhna računalniška podjetja, kot sta Troy's Computers in servis My Florida PC.

Kljub resnosti obtožb pa obstajajo določeni dvomi glede samega razpleta na sodišču, saj primer odpira že znano pravno problematiko. Podobna tožba iz leta 2018 je bila namreč na istem sodišču zavrnjena, saj je prizivno sodišče leta 2022 odločilo, da je bilo ravnanje trojice bolj verjetno posledica zakonitega, čeprav vzporednega tržnega obnašanja v panogi, v kateri prevladujejo le trije dobavitelji. Tokratni tožniki upajo, da bo prav hiter prehod na HBM služil kot ključni dodatni dokaz o dejanskem usklajevanju. Obtožena podjetja sicer javno zatrjujejo, da delujejo neodvisno, na samo tožbo pa uradno še niso odgovorila. Omeniti velja, da bi se lahko cene sistemskih pomnilnikov v tretjem četrtletju dvignile še za 40 do 50 %, v zadnjem pa za dodatnih 30 do 40 % brez izboljšanja pred letom 2028.

Nič več stekla v optičnih kablih?

Podjetja China Telecom, Yangtze Optical Fibre and Cable ter Dekoli so združila moči pod okriljem kitajske nacionalne raziskovalne pobude in izvedla prenos podatkov po optičnem kablu z votlim jedrom, ki postavlja povsem nova merila v industriji. Z uporabo optimiziranega prenosnega sistema je ekipa dosegla skupno zmogljivost 51,3 Tb/s prenosa na razdalji približno 206 km, in to brez uporabe signalnih ojačevalnikov med potjo. Preizkus je za nameček potekal na najdaljšem komercialnem čezmejnem kablu z votlim jedrom na svetu.

Za razliko od tradicionalnih optičnih kablov, kjer svetloba potuje skozi steklo, se pri tej novi tehnologiji svetlobni signali širijo po zraku znotraj votlega jedra. Takšna zasnova odpravlja fizikalne omejitve klasičnega stekla, zmanjšuje signalni zamik in opazno povečuje pasovno širino. Zara-

di teh lastnosti se optična vlakna z votlim jedrom uveljavljajo kot ključna tehnologija prihodnjih hrbteničnih omrežij in velikih podatkovnih centrov.

Pri tem velja omeniti, da visokozmogljiv prenos podatkov v realnem okolju zunaj laboratorija prinaša številne izzive pri zagotavljanju stabilnosti, ki jih bo treba dolgoročno rešiti. Kitajski inženirji so sicer stabilnost poskušali rešiti z uvedbo prilagodljivega mehanizma za nadzor hitrosti in s prožnim dodeljevanjem moči kanalom. Sistem tako dinamično prilagaja prenos podatkov za vsako valovno dolžino posebej, kar omogoča hibridno delovanje z različnimi hitrostmi in nastavitvami.

Pomemben del sistema je tudi nova arhitektura ojačevalnika, ki z dvema ojačitvenima stopnjama zagotavlja stabilen signal in največjo izhodno moč 33,5 dBm (približno 2,2 W optične moči). Ker gre za visoke vrednosti, so v sistem vgradili napredne varovalne mehanizme. Ti vključujejo neprekinjeno spremljanje stabilnosti, samodejni izklop ob zaznavi nevarnih pogojev ter alarmne sisteme. Ti ukrepi hitro prepoznajo nepravilnosti, s čimer preprečujejo poškodbe drage opreme in povečujejo zanesljivost celotnega omrežja.

Microsoft postaja največje razočaranje borzne zgodbe

Ko govorimo o največjih zmagovalcih umetne inteligence na borzi, se običajno omenjajo Nvidia, Alphabet ali Meta. Manj pozornosti pa dobiva Microsoft – podjetje, ki je bilo zaradi tesnega sodelovanja z OpenAI še pred kratkim simbol revolucije umetne inteligence. Letos se je slika močno spremenila.

Microsoftove delnice so od začetka leta izgubile približno četrtino vrednosti, podjetje pa je med t. i. "Magnificent 7" trenutno najmanj uspešno tehnološko podjetje. Samo letos je iz njegove tržne kapitalizacije izpuhtelo okoli 857 milijard dolarjev. Na prvi pogled je padec presenetljiv.

Microsoft ima vodilno platformo Azure, enega največjih poslovnih ekosistemov na svetu, lastnega UI pomočnika Copilot ter je tesno povezan z OpenAI.

Toda vlagateljev to trenutno ne prepriča. Razlog je dvojni pritisk, ki ga občuti podjetje. Po eni strani Microsoft vlaga rekordne zneske v čipe, gradnjo UI infrastrukture ter podatkovnih centrov. Po drugi strani pa se pojavlja vse več vprašanj, kako bo umetna inteligenca vplivala na njegov glavni posel – prodajo programske opreme. Microsoft se je tako znašel v nenavadnem položaju. Podjetje želi biti eden glavnih ponudnikov umetne inteligence, hkrati pa prav ta ista UI ogroža številne tradicionalne programske izdelke, na katerih temelji njegov poslovni model. Vlagatelji se zato sprašujejo, ali bodo ogromne investicije dovolj hitro prinesle nove

prihodke ali pa bo UI prej zmanjšala vrednost obstoječih programskih rešitev. Gre za dilemo, s katero se trenutno sooča le malo drugih tehnoloških velikanov. Še pred letom dni je trg skoraj brez pomislekov nagrajeval vsako podjetje, ki je napovedalo večje investicije v umetno inteligenco. Danes je razpoloženje drugačno, saj vlagatelji vse bolj zahtevajo konkretne rezultate. Visoki kapitalski izdatki sami po sebi niso več dovolj. Trg želi videti rast prihodkov in dobičkonosnost. Microsoft zato občuti pritisk z obeh strani: visoki stroški rastejo, donosnost teh vlaganj pa ostaja dolgoročnejša zgodba.

Podobne izzive trenutno doživlja tudi Oracle, ki prav tako intenzivno vlaga v UI infrastrukturo in podatkovne centre. Obe podjetji sta se znašli v položaju, kjer vlagatelji podpirajo dolgoročno strategijo, vendar dvomijo o kratkoročnem finančnem učinku tako velikih investicij.

To kaže, da se trg umetne inteligence premika v novo fazo. Prvo obdobje je bilo zaznamovano z navdušenjem. Drugo zaznamujejo vprašanja o donosnosti.

Kljub padcu vrednosti delnice Microsofta nekateri vlagatelji ostajajo optimistični. Med njimi je tudi Michael Burry, vlagatelj, ki je zaslovel z napovedjo finančne krize leta 2008. Burry je razkril, da stavi na dolgoročno rast Microsoftovih delnic, in sicer z nakupom opcij, ki zapadejo leta 2028. Po njegovem mnenju je trenutno vrednotenje podjetja precej nižje od njegovega dolgoročnega potenciala.

To kaže, da del trga sedanji padec razume kot priložnost in ne kot znak trajnejših težav.

Microsoft ostaja eno najmočnejših tehnoloških podjetij na svetu. Toda letošnje dogajanje kaže, da sama prisotnost na področju umetne inteligence vlagateljem ni več dovolj. Trg vse bolj razlikuje med podjetji, ki obljubljajo prihodnost, in podjetji, ki jo že pretvarjajo v dobiček.

Za Microsoft bo zato naslednjih nekaj četrtletij ključnih. Moral bi dokazati, da zna razvijati umetno inteligenco, predvsem pa, da zna z njo ustvarjati večjo vrednost za delničarje.

Poceni spletni nakupi izven EU so postali dražji

Spletni nakupi iz trgovin, ki blago pošiljajo iz držav izven Evropske unije, niso več tako brezskrbni kot so bili še pred dnevi. Od 1. julija 2026 namreč velja spremenjena carinska ureditev, po kateri se tudi za pošiljke manjše vrednosti (do 150 evrov) obračuna začasna carinska dajatev v višini treh evrov.

Največjo spremembo bodo občutili kupci, ki pogosto naročajo izdelke manjših vrednosti iz spletnih trgovin, kot so AliExpress, Temu, Shein, Alibaba, eBay ali drugih platform, kjer blago pogosto prispe neposredno iz Kitajske oziroma drugih držav izven EU. Do zdaj so bile takšne pošiljke do vrednosti 150 evrov oproščene carine, po novem pa to ne velja več.

Za potrošnika je pomembno, da trije evri ne pomenijo nujno treh evrov na celotno naročilo. Dajatev se obračuna na posamezno postavko oziroma vrsto blaga v carinski deklaraciji. Če je v paketu pet enakih majic, gre praviloma za eno postavko in znesek nanese tri evre. Če pa so v paketu majica, dežnik in čevlji, lahko to pomeni tri različne postavke in skupaj devet evrov carinske dajatve.

Poleg nove carinske dajatve se seveda še naprej obračunava tudi DDV. To pomeni, da se lahko pri zelo poceni izdelkih končna cena hitro občutno zviša. Če na primer kupec naroči majico za 10 evrov, se najprej obračuna tri evre carine, nato pa se DDV obračuna od davčne osnove, v katero je vključena tudi carina. Pri 22-% DDV-ju bi to pomenilo dodatnih 2,68 evra davka, skupaj torej 5,68 evra dodatnih stroškov.

Nova ureditev velja za blago, ki se ob naročilu nahaja izven Evropske unije. Če je izdelek že v Sloveniji ali v drugi državi EU, začasne carinske dajatve ni treba plačati. To pa ne pomeni, da je dovolj, da ima spletna trgovina evropsko domeno ali slovensko prevedeno spletno stran. Pomembno je, od kod je blago dejansko odpremljeno.

Pred 1. julijem so bili kupci dodatno zmedeni, saj niso bili prepričani, ali je – da se izognejo novemu sistemu – dovolj, da naročilo ustvarijo pred 1. julijem (na primer 30. junija). Seveda ni bil merodajen datum naročila, temveč datum sprejetja carinske deklaracije oziroma carinjenja pošiljke. To pomeni, da se je lahko nova dajatev obračunala tudi za paket, ki je bil naročen pred 1. julijem, vendar je bil v carinski postopek sprejet šele po tem datumu. Sprememba vpliva tudi na vračila. Pri prodaji na daljavo do vrednosti 150 evrov se odpravlja možnost razveljavitve carinske deklaracije zgolj zaradi vračila blaga, zato vračilo plačanih dajatev ne bo več samoumevno. Povračilo bo mogoče predvsem v primerih, ko bo blago pomanjkljivo ali ne bo izpolnjevalo pogojev iz pogodbe.

Cilj nove ureditve je omejiti množični uvoz nizkocenovnih paketov iz tretjih držav, ob katerem so evropski trgovci pogosto v neenakem položaju. Ti morajo izpolnjevati evropske zahteve glede varnosti, skladnosti, davkov, vračil in odgovornosti za izdelke, medtem ko so številni prodajalci izven EU dolga leta izkoriščali ugodnejši režim za majhne pošiljke.

Nova pravila verjetno ne bodo ustavila nakupovanja na Temuju, Sheinu ali AliExpressu – največ, za kar si Evropa lahko prizadeva je, da se število pošiljk zmanjša in s tem poveča možnost, da se bodo potrošniki zaradi višjih cen mogoče raje odločili za lokalnega ponudnika.

Fizične igre za Xbox bi spremenili v digitalne

Microsoft naj bi pripravljal novo funkcijo za konzole Xbox, s katero bi lahko uporabniki svoje fizične igre na ploščkih pretvorili v digitalno zbirko. Gre za rešitev, ki bi lahko postala zelo pomembna pri prihodnjih generacijah konzol, še posebej, če se bo industrija dokončno začela poslavljati od fizičnih nosilcev iger.

Microsoft naj bi funkcijo interno že testiral med zaposlenimi. Namigi o možnosti »Disc2Digital« so se sicer že pred časom pojavili tudi v kodi aplikacije Xbox za osebne računalnike. Nova možnost naj bi bila namenjena predvsem lastnikom iger za Xbox One in Xbox Series X, medtem ko naj ne bi bili podprti ploščki za Xbox 360 in izvirni Xbox. Postopek naj bi bil za uporabnika precej preprost. Igro bi vstavil v konzolo, jo namestil in zagnal, sistem pa bi mu ob tem dodelil digitalno pravico do uporabe igre. Ta pravica bi bila vezana na Microsoftov račun in na konkretni fizični plošček. To pomeni, da bi igra tudi po digitalizaciji ostala povezana z originalnim nosilcem, tako da uporabnik vseeno ne bi dobil popolnoma neodvisne digitalne kopije. To pomeni, da bi se v primeru, da bi uporabnik plošček posodil prijatelju ali ga prodal, z njim prenesla tudi digitalna pravica. S tem bi Microsoft preprečil, da bi uporabniki en fizični izvod igre trajno pretvorili v več ločenih digitalnih kopij.

Takšen pristop digitalizacije iger bi lahko rešil eno večjih težav prehoda v popolnoma digitalno prihodnost. Veliko uporabnikov ima namreč doma obsežne zbirke fizičnih iger za Xbox, od katerih se ne želijo posloviti zgolj zato, ker bodo prihodnje konzole morda brez optičnega pogona. Če bi Microsoft funkcijo res uvedel, bi lahko igralcem omogočil lažji prehod na novejše naprave, hkrati pa ohranil vrednost obstoječih zbirk, saj bi fizični ploščki tudi po tem ostali uporabni. Digitalna pravica bi v praksi delovala podobno kot nakup igre v Microsoftovi spletni trgovini. Če bi bila igra del storitve Xbox Cloud Gaming in bi imel uporabnik naročnino Game Pass, bi jo lahko pretakal iz oblaka. Če bi šlo za igro Xbox Play Anywhere, bi bila igra lahko dostopna tudi na osebnih računalnikih in ročnih igralnih napravah. Funkcija naj bi podpirala tudi igre, ki so bile priložene konzolam, ter igre na več ploščkih. V določenih primerih bi lahko omogočila tudi dostop do dodatnih vsebin, ki so bile sicer vključene na originalnem mediju. Vendar naj bi Microsoft testerje že opozoril, da vsi ploščki za Xbox One morda ne bodo združljivi, saj je podpora odvisna tudi od načina in časa izdelave posameznega diska. Za zdaj je funkcija, kot rečeno, v fazi internega testiranja, zato je Microsoft še ni uradno predstavil.

Ste si v Whatsappu že rezervirali svoje uporabniško ime?

WhatsApp pripravlja novost, ki bo uporabnikom omogočila več zasebnosti pri dodajanju novih stikov in začetku pogovorov. Namesto da bi mo-

rali z nekom za začetek pogovora deliti svojo telefonsko številko, kot je bilo do zdaj, bodo lahko imeli uporabniki za ta namen svoje uporabniško ime. Funkcijo naj bi uradno uvedli še letos, njen glavni namen pa je zmanjšati potrebo po razkrivanju osebnih telefonskih številk ljudem, ki jih uporabnik še nima shranjenih med stiki.

Novost bo še posebej uporabna v primerih, ko bo želel uporabnik vzpostaviti stik z nekom, ki mu ne bo želel takoj razkriti svoje telefonske številke. To lahko pride prav pri spletnih nakupih, komunikaciji z neznanci, začasnih dogovorih, skupnostih, službenih stikih ali drugih situacijah, kjer je telefonska številka pogosto preveč oseben podatek.

WhatsApp bo uporabniška imena uvajal postopoma, vendar je rezervacija imen že na voljo v aplikaciji. Uporabniki lahko tako rezervirajo želeno uporabniško ime, še preden bo funkcija pogovorov prek uporabniškega imena dejansko omogočena. S tem želi WhatsApp uporabnikom dati dovolj časa, da si zagotovijo ime, ki ga morda že uporabljajo na drugih platformah.

Pri WhatsAppu poudarjajo, da ima storitev več kot tri milijarde uporabnikov, zato je pri imenih pričakovati veliko »prekrivanja«. Prav zato rezervacije odpirajo predčasno, da bi imeli uporabniki več možnosti pravočasno izbrati želeno ime – sicer pa: kdor prvi pride, prvi melje.

Postopek rezervacije bo odvisen od naprave. Uporabniki Androida bodo lahko uporabniško ime nastavili v najnovejši različici aplikacije prek poti Nastavitve > Račun/Profil > Uporabniško ime. Na iPhonu bo treba odpreti razdelek »You«, izbrati profil in nato možnost za ustvarjanje uporabniškega imena.

WhatsApp bo posameznikom in organizacijam omogočil tudi uporabo obstoječih imen z Instagrama ali Facebooka, če ta še niso zasedena. Pri tem pa bo podjetje posebej previdno pri znanih osebah. Nekatera uporabniška imena, povezana s slavnimi osebnostmi, politiki in drugimi javno prepoznavnimi osebami, so že vnaprej zaščitena, da jih ne bi prevzeli drugi uporabniki. To pomeni, da bodo morali nekateri uporabniki z enakim imenom kot znana oseba izbrati drugačno različico. Pomembno pa je, da WhatsApp uporabniških imen ne bo spremenil v klasičen javni imenik. Uporabnikov ne bo mogoče preprosto iskati po imenih. Za začetek pogovora bo treba poznati natančno uporabniško ime osebe, s katero želite stopiti v stik. S tem želi WhatsApp preprečiti množično iskanje oseb, nadlegovanje in neželena sporočila.

Nova zasebnostna zaščita bo veljala predvsem za nove pogovore. Če ste svojo telefonsko številko že delili z obstoječimi stiki ali ste z njimi v skupinskih pogovorih, bo številka zanje še vedno vidna. Poleg uporabniških imen WhatsApp pripravlja še dodatno možnost, imenovano »username key«. Gre za izbirni varnostni ključ, ki ga bo moral poznati vsak, ki bo želel stopiti v stik z vami prek uporabniškega imena.

Konec digitalnega lastništva? Sony briše več kot 550 filmov

Podjetje Sony bo s 1. septembrom 2026 iz računov svojih strank na platformi PlayStation popolnoma odstranilo vse filme in televizijske oddaje produkcijske hiše Studio Canal. Razlog za to radikalno potezo se skriva v preteku licenčnih pogodb. Oškodovani uporabniki ob tem nimajo nobene možnosti, da bi vsebine prenesli na druge naprave za ogled brez spletne povezave, Sony pa jim prav tako ne bo vrnil denarja. To je v spletnih forumih nemudoma obudilo znani pregovor: »Če nakup ne pomeni lastništva, potem piratstvo ni kraja.«

V tej luči se je znova obudila resničnost legendarne izjave soustanovitelja podjetja Valve, Gabea Newella, iz leta 2011, ki je poudaril, da piratstvo ni vprašanje cene, temveč kakovosti storitve. Newell je takrat pojasnil, da je ponudba vrhunske in zanesljive storitve najboljše orožje proti piratstvu. Če pa »nakup« digitalne vsebine pomeni le dostop za nedoločen čas, ki je povsem odvisen od nestanovitnih korporativnih pogodb, potem je takšen sistem problematičen že v samem temelju. Povsem logično je, da bodo uporabniki začeli iskati alternative drugje.

To kar počne Sony, je enakovredno situaciji, v kateri bi vam nekdo prodal fizični DVD, nato pa vam po nekaj letih vlomil v hišo in ga odnesel. Sonyjeva pravna služba se bo vsekakor skliceva-

la na splošne pogoje uporabe, v katerih piše, da si pridržujejo pravico do preklica dostopa. Vendar pa je takšno opravičilo precej za lase privlečeno. Potrošniki so namreč ob prevzemu vsebin kliknili gumb, na katerem je jasno pisalo »Kupi« (Buy) in ne »Najemi« (Rent). Tudi v uradnem obvestilu o izbrisu Sony sam uporablja izraz »predhodno kupljene vsebine«.

Meta zaklepa funkcije pametnih očal

Uporabniki pametnih očal Ray-Ban Meta druge generacije bodo morali v prihodnje seči globlje v žep, če bodo želeli nemoteno uporabljati vse zmogljivosti te nosljive tehnologije. Podjetje Meta namreč uvaja nov naročniški paket Meta One Premium, ki bo stal približno 18 evrov mesečno. Podjetje to spremembo uvaja prek sistema mesečnih omejitev porabe oziroma tako imenovanih »kapic«, ki bodo drastično skrajšale čas brezplačne uporabe določenih naprednih možnosti. Prva funkcija, ki se je znašla na udaru teh strogih omejitev, je izboljšanje zvoka pogovora. Gre za uporaben sistem, ki v slušalkah očal inteligentno ojača oziroma poviša glas osebe, s katero se lastnik očal pogovarja, s čimer znatno olajša razumevanje v hrupnem okolju. Brez plačane naročnine bo ta možnost po novem na voljo zgolj za tri ure na mesec. Tudi tisti, ki se bodo odločili za plačevanje premijskega paketa, ne bodo imeli neomejenega dostopa, saj bo uporaba v vsakem primeru omejena na 15 ur mesečno.

Celoten proces ostrenja pogovora sicer poteka lokalno na samih očalih in deluje povsem brez internetne povezave. To pomeni, da Meta z zaračunavanjem te storitve ne pokriva stroškov vzdrževanja zunanjih strežnikov ali prenosa podatkov. Namesto tega so se v podjetju odločili, da za »naročniški zid« zaklenejo funkcijo, ki jo vgrajena strojna oprema očal že sama po sebi brez težav obvladuje. Tovrstno ravnanje upravičeno vzbuja precejšnjo skrb med potrošniki, saj postavlja pod vprašaj smiselnost nakupa naprave, katere lastnosti se lahko naknadno poljubno zaklenejo. Dodatno mero nejevolje povzroča tudi dejstvo, da program sploh ne ponuja možnosti vpogleda preostalega razpoložljivega časa znotraj tekočega meseca. Če uporabnik svojih ur ne porabi, se te tudi ne prenesejo v naslednji mesec, temveč nepovratno zapadejo.

Prvi prilagodljivi čip AMD z integriranim pomnilnikom

Podjetje AMD se je na izzive z nepredvidljivimi nihanji cen pomnilniških modulov odzvalo s precej zanimivim arhitekturnim »premikom«. Namesto zanašanja na drage in težko dostopne module HBM ali klasične zunanje pomnilnike DRAM, so v svoj najnovejši prilagodljivi čip Versal Premium Gen 2 neposredno vgradili pomnilniško rešitev MoP (Memory on Package). Gre za pristop, ki integrira do štiri pomnilniška vezja LPDDR5X neposredno v samo ohišje procesorja, s čimer se odpravlja potreba po zapletenem načrtovanju in usmerjanju povezav na matični plošči. Novi model prinaša izjemno visoko stopnjo integracije, saj ponuja sistemski pomnilnik do kapacitete 32 GB s hitrostmi delovanja do 9.000 MT/s, kar v praksi pomeni prepustnost podatkov do 288 GB/s. Ta rešitev ne izboljšuje le zmogljivosti, temveč prinaša ključno prednost pri optimizaciji prostora. Ker zunanji pomnilniški čipi niso več potrebni, se površina, ki jo vezje zaseda na sistemski plošči, zmanjša za več kot 60 odstotkov. To pa odpira vrata za uporabo čipov v izjemno kompaktnih industrijskih formatih, kot sta EDSFF ali 3U VPX, kjer so prostorske in temperaturne omejitve izjemno stroge. Ker pa gre za nov in razmeroma nišen pristop na področju prilagodljivih čipov SoC (System on a Chip), trenutno še ni znano, kako dobro se bo ta integrirana arhitektura obnesla pri dolgotrajnih, specifičnih obremenitvah zunaj idealnih laboratorijskih pogojev. Kar zadeva preostale tehnične lastnosti, Versal Premium Gen 2 MoP temelji na procesorski arhitekturi Arm in prinaša do 10-krat večjo računsko moč v primerjavi s prvo generacijo. Vgrajena je strojna podpora za najnovejša protokola CXL 3.1 in PCIe 6.0 s hitrostjo prenosa podatkov do 64 Gb/s, kar omogoča bliskovito komunikacijo ob združevanju s procesorji AMD EPYC. Posebna pozornost je bila namenjena varnosti in trajnosti. Čip vključuje strojno šifriranje podatkov v mirovanju (DDR) ter napredne 400G kriptografske motorje, ki ščitijo podatke pred fizičnimi napadi na povezovalnem nivoju, ne da bi ob tem trpela splošna prepustnost sistema. Ker so te naprave namenjene zahtevnim industrijskim okoljem, telekomunikacijam in sistemom za obrambo, podjetje AMD zagotavlja visoko odpornost pri delovanju v temperaturnem razponu od -40 °C do 110 °C ter izjemno dolg življenjski cikel, ki presega 15 let.

Huawei Watch Fit 5 Pro: ura, ki je prerasla športno zapestnico

TESTIRAMO

Huawei Watch Fit 5 Pro je ura, ki bo zadoščala večini uporabnikov. V primerjavi s predhodnico je dobila tudi nekaj nadgradenj, ki pa drastično ne spremenijo izkušnje.

Že lansko leto sem rekel, da je Watch Fit 4 Pro ura, ki bo zadoščala potrebam 90 % uporabnikov. Enako velja tudi za novo Huawei Watch Fit 5 Pro, ki pa je zame bolj prehodna ura, saj prelomnih nadgradenj ni bila deležna.

Huawei Watch Fit 5 Pro – oblika ostaja kvadratna, ampak deluje odraslo

Že v članku o Watch Fit 5 sem napisal, da kvadratna oblika ne bo všeč vsakomur. Sam se še vedno bolj nagibam k okroglim uram, ker na zapestju delujejo bolj klasično, pogosto bolj elegantno in manj očitno posnemajo Apple. Ampak pri Watch Fit 5 Pro bi težko rekel, da oblika ne deluje. Zdi se mi, da je Huawei kvadratno osnovo dobro izkoristil.

Velik zaslon je pri takšni obliki bolj uporaben kot pri okrogli uri. Obvestila so bolj pregledna, zemljevidi imajo več smisla, vadbeni podatki so razporejeni bolj naravno, tudi meniji se berejo hitreje. Pri okroglih urah je del zaslona vedno v določeni meri žrtev oblike. Pri Watch Fit 5 Pro tega občutka ni. Ohišje meri 44,5 × 40,8 × 9,5 milimetra, masa ure brez paščka pa je 30 gramov. To je še vedno dovolj lahkotno, da ura ne moti med spanjem ali telovadbo.

Glavna razlika v primerjavi z navadno Watch Fit 5 so materiali. Spredaj je 2,5D safirno steklo, okoli zaslona je titanov okvir, ohišje pa je aluminijasto. Bela različica ima še posebno obdelavo s plazemsko elektrolitsko oksidacijo, ki ustvari bolj trdo, keramiki podobno površino. Na papirju se vse to sliši zelo premijsko. Na zapestju razlika ni tako dramatična, kot bi si Huawei morda želel, vendar obstaja. Pro deluje bolj čvrsto, bolj zrelo in manj kot športna zapestnica.

Zaslon je eden najboljših razlogov za Pro različico

Zaslon je pri Watch Fit 5 Pro tisti del, kjer sem najhitreje razumel, zakaj Huawei za Pro želi več denarja. Gre za 1,92-palčni AMOLED LTPO zaslon z osveževanjem od 1 do 60 Hz in svetilnostjo do 3000 nitov.

Že pri navadni Watch Fit 5 sem bil z zaslonom zelo zadovoljen. Pro gre še korak dlje. Ne toliko zaradi barv, ker so bile že prej odlične, ampak zaradi kombinacije svetilnosti, tankih robov in občutka, da se vse dogaja tik pod prstom. Robovi so tanki, zaslon zapolni velik del sprednje strani in zaradi kvadratne oblike res dobiš občutek, da je površine veliko.

LTPO osveževanje je dobrodošlo predvsem zaradi baterije. Ura lahko pri statičnem prikazu pade na zelo nizko raven osveževanja slike, pri premikanju po menijih pa ostane prikaz dovolj tekoč.

Sistem je hiter, ampak še vedno ne tako pameten kot Wear OS ali drugi

Huawei uporablja HarmonyOS in aplikacijo Huawei Zdravje. Namestitev je razmeroma preprosta, tudi če uporabljate Android telefon, ki ni Huawei. Pri iPhonu deluje osnovna sinhronizacija, obvestila in športni podatki, vendar je zaradi Applovih omejitev izkušnja bolj zaprta. To ni nova zgodba in tudi ni izključno Huaweieva krivda.

Vmesnik je pregleden. Zgornji gumb oziroma krona odpre meni, spodnji gumb lahko uporabite za bližnjice, najpogosteje do športnih načinov. Vrtenje krone je dobro odzivno in prijetno, haptika pa dovolj močna, da jo opaziš. Na uri lahko sprejemaš klice prek Bluetooth povezave, uporabljaš mikrofon in zvočnik, nastavljaš alarme, preveriš vreme, upravljaš glasbo, uporabljaš snemalnik zvoka, kompas, svetilko, časovnik in še nekaj drugih orodij.

Vendar je treba biti pošten. To ni ura za uporabnika, ki želi polno pametno izkušnjo z aplikacijami, Google storitvami, neodvisnimi zemljevidi, naprednimi integracijami, bogato trgovino in LTE povezavo. AppGallery na uri obstaja, vendar izbira aplikacij ni primerljiva z Apple Watch ali Wear OS. Nekatere stvari so uporabne, na primer Curve Pay za brezstično plačevanje, Petal Maps za zemljevide ali različne športne aplikacije, ampak občutek je bolj omejen.

Huawei in šport že od nekdaj sodita skupaj

Huawei se najbolje znajde pri športnih funkcijah. Več kot 100 športnih načinov je danes že skoraj kliše, ker jih ima vsaka druga ura. Pomembnejše je, kaj ura naredi pri športnih merjenjih, ki jih ljudje dejansko uporabljajo. Pri Watch Fit 5 Pro so najbolj zanimivi tek, kolesarjenje, trail tek, golf, plavanje oziroma potapljanje na dah in športi z loparjem.

Pri teku prejmete običajne podatke o tempu, srčnem utripu, porabljenih kalorijah, conah intenzivnosti, VO2 Max, regeneraciji in drugih metrikah. Pri trail teku ura pokaže naklon, višino, razdaljo, oceno preostale poti, opozorila ob odmiku s trase in podporo za zemljevide. V »trail« načinu Huawei Watch Fit 5 Pro zdrži do 25 ur, kar je več kot dovolj, da pretečeš celotno zastavljeno pot.

GPS je bil pri zadnjih Huawei urah že dober, pri Watch Fit 5 Pro pa se opira na njihov Sunflower Positioning System oziroma naprednejšo anteno in algoritme. To pomeni manj tistih čudnih ovinkov po zemljevidu, ko ura misli, da ste tekli skozi stavbo ali čez cesto, kjer vas ni bilo. Seveda pri urbanih kanjonih, gozdovih in slabem vremenu nobena ura ni popolna, ampak Huawei je tu med bolj zanesljivimi.

Kolesarjenje je dobilo veliko pozornosti. Ura lahko spremlja naklon, virtualno moč in virtualno kadenco, telefon pa lahko služi kot večji zaslon oziroma kolesarski računalnik. Če imate zunanji merilnik moči, se lahko povežete tudi z njim in spremljate FTP. To ni nadomestilo za resen Garmin ali Wahoo kolesarski računalnik za zahtevne kolesarje, je pa zelo dobra rešitev za rekreativce, ki ne želijo kupiti še ene naprave. Golf funkcije so zanimive, če jih boste res uporabljali.

Kratke vadbe bodo za nekoga uporabne, za drugega pač ne

To je zdaj moj drugi poskus s kratkimi vadbami. Še enkrat, ideja ni slaba, tudi izvedba je prava, ampak sprašujem se, kako uporabne so zares te kratke vadbe.

Huawei je vključil 30 animiranih gibov za 10 delov telesa, med drugim za vrat, ramena in hrbet. Vse skupaj je zapakirano v bolj igrivo obliko s pando, ki te spodbuja k raztezanju.

Da, malo otročje je. In da, odrasel človek verjetno ne potrebuje pande, da vstane s stola. Vseeno pa ti majhni opomniki mogoče komu pridejo prav.

Veliko podatkov, a ura ni zdravnik na zapestju

Huawei je pri zdravstvenih meritvah zelo agresiven. Watch Fit 5 Pro meri srčni utrip, SpO2, stres, temperaturna nihanja, HRV, spanje, dremeže, čustveno počutje, menstrualni cikel, ponuja EKG, analizo arterijske togosti, analizo aritmije pulznega vala in spremljanje dihanja med spanjem. To je za uro v tem cenovnem razredu zelo bogat paket in glavni razlog, da sem že lansko leto rekel, da ne potrebuješ dražje ure.

EKG se izvede tako, da 30 sekund držite prst na stranski elektrodi. Analiza aritmije pulznega vala uporablja PPG senzor in lahko opozarja na morebitna tveganja, povezana z atrijsko fibrilacijo.

Vse to se sliši zelo resno, zato je treba dodati najpomembnejše opozorilo: ura ni medicinska diagnoza. Če ura pokaže nekaj nenavadnega, je to lahko razlog za posvet z zdravnikom, ne pa razlog za samodiagnosticiranje.

Spremljanje spanja je uporabno, vendar ga ne bi jemal kot absolutno resnico.

Baterija je pri Huaweiu vedno močna točka

Zdrži do 10 dni, če si skromen, 6 dni ob vsakodnevni telovadbi in z vsemi vklopljenimi meritvami in 3-4 dni, če boš imel vedno vklopljen zaslon. Vse številke so odlične in boljše od večine ur drugih proizvajalcev, pri katerih moraš o polnjenju razmišljati vsak drugi dan, še vedno pa močno zaostajajo pred avtonomijo, ki jo nudijo njihove ure Huawei Watch GT 6.

Polnjenje traja okoli eno uro, kar je dovolj hitro. Magnetni polnilnik je klasična rešitev, a želel bi si, da bi Huawei pri takšni uri še bolj standardiziral polnjenje ali vsaj poskrbel, da bi bil kabel bolj univerzalen.

Motijo me malenkosti, ki jih lahko zlahka popravijo

Najprej me moti dolgoročna podpora. Huawei bi moral pri urah jasneje povedati, koliko let bo posamezna serija prejemala nove funkcije, plačilno podporo in pomembne nadgradnje. Pri telefonih smo se navadili na konkretne obljube, pri urah pa je še vedno preveč nejasnosti.

Druga stvar je cena. 299 evrov ni nerazumno glede na materiale in funkcije, vendar Watch Fit 5 Pro ni več impulzni nakup. Navadna Watch Fit 5 je za večino dovolj dobra. Pro je smiselna, če res želite boljši zaslon, safirno steklo, boljše materiale, naprednejše športne funkcije, EKG in dodatne zdravstvene meritve. Če boste uro uporabljali samo za obvestila, štetje korakov, meritve spanca in občasno hojo, je Pro skoraj preveč.

Na tretje mesto bi dal ekosistem. Huawei Health je dobra aplikacija, ura je odzivna, podatkov je ogromno, vendar se pri aplikacijah tretjih ponudnikov (stanje se je izboljšalo v zadnjih letih), plačilih in integracijah hitro pokaže, da Huawei ni Apple, Google ali Samsung. Curve Pay je super za plačila in jih je rešil potem, ko so izgubili poljskega ponudnika, ampak zamerim jim, da so podporo za brezstično plačevanje omejili na letošnje in lanske generacije naprav. Premijske ure izpred dveh let niso dobile podpore za Curve Pay.

Skratka, Huawei Watch Fit 5 Pro je zelo dobra ura. Morda celo najbolj prepričljiva ura v seriji Watch Fit do zdaj.

Watch Fit 5 Pro bi priporočil tistim, ki ne potrebujejo ure za 500-700 evrov, a tudi nočejo več nositi plastične zapestnice z majhnim zaslonom.

Evropa mora pospraviti svojo digitalno hišo, ne da bi prodala temelje

Evropa ima zanimiv odnos do pravil. Radi jih imamo.

Foto: Pixabay

Ko se pojavi nov družbeni ali tehnološki izziv, pogosto najprej ustanovimo strokovno skupino, pripravimo strategijo, odpremo javno posvetovanje, napišemo uredbo, sprejmemo izvedbene akte in nato ustanovimo še organ, ki preverja izvajanje vseh teh pravil. Takšen pristop je včasih predmet šal, vendar ima tudi zelo pomembno prednost: Evropa je zaradi njega ustvarila enega najbolj varnih in zaupanja vrednih prostorov na svetu.

Tehnološka tekma

Prav evropski pristop je zagotovil, da digitalni razvoj ni razumljen samo kot tehnološka tekma, ampak tudi kot vprašanje družbe, človekovih pravic in vrednot. Evropska ideja je vedno temeljila na prepričanju, da mora tehnologija služiti človeku in ne človek tehnologiji. In to ni nepomembno. V času, ko algoritmi odločajo, katere informacije vidimo, umetna inteligenca vpliva na poslovne procese, podatki pa so postali ena najpomembnejših gospodarskih surovin, vprašanje pravil ni več birokratsko vprašanje. Je vprašanje tega, v kakšni digitalni družbi želimo živeti. Toda vsaka uspešna zgodba potrebuje tudi trenutek iskrene presoje. Po desetletju izjemno intenzivnega sprejemanja digitalne zakonodaje se mora Evropa vprašati nekaj zelo preprostega: ali smo zgradili digitalno avtocesto prihodnosti ali pa smo ob njej postavili toliko prometnih znakov, da voznik več časa namenja branju navodil kot sami vožnji?

Jaka Repanšek, vodja Strateške skupine za digitalno regulativo pri Slovenski digitalni koaliciji in sopredsedujoči AmCham komisije za intelektualno lastnino in digitalno regulativo.

Omnibus in evropski standardi

Prav zato je razprava o digitalnem omnibusu Evropske unije tako pomembna. Ne zato, ker bi bila evropska digitalna regulacija napačna. GDPR je postal globalni standard varstva osebnih podatkov. Akt o digitalnih storitvah (DSA) je postavil pomembna pravila odgovornosti spletnih platform. Akt o digitalnih trgih (DMA) odpira vprašanje pravične konkurence v digitalnem gospodarstvu. Akt o umetni inteligenci (AI Act) je prvi celovit horizontalni okvir za urejanje umetne inteligence na svetu. K temu lahko dodamo še Data Act, Data Governance Act, direktivo NIS2 in številne druge predpise.

Evropa je tako nedvomno postala regulatorna velesila digitalnega sveta. Toda naslednje desetletje ne bo odločalo vprašanje, kdo zna napisati največ pravil. Odločalo bo vprašanje, kdo zna napisati najboljša pravila.

Digitalni omnibus mora zato pomeniti prehod od več regulacije k boljši regulaciji. To ni projekt rušenja evropskih standardov. To ni odpoved zasebnosti, varnosti ali temeljnim pravicam. Ravno nasprotno. Gre za vprašanje, kako te vrednote zaščititi na način, ki bo deloval tudi v realnem svetu hitrih tehnoloških sprememb. Beseda deregulacija ima v Evropi pogosto skoraj negativen prizvok. Marsikdo jo razume kot manj zaščite, manj odgovornosti ali manj pravic. Toda pametna deregulacija pomeni nekaj povsem drugega: odstraniti nepotrebno kompleksnost zato, da lahko bolje zaščitimo bistvo. Predstavljajmo si evropsko podjetje, ki razvija umetno inteligenco za pomoč zdravnikom pri zgodnejšem odkrivanju bolezni. Ekipa ima znanje, tehnologijo in idejo, ki lahko pomaga ljudem. Toda že v začetni fazi mora razumeti zahteve AI Acta, GDPR, pravil o podatkih, kibernetski varnosti, medicinski zakonodaji in različnih nacionalnih interpretacijah. Vsa ta področja so pomembna. Nihče si ne želi umetne inteligence v zdravstvu brez nadzora. Toda vprašanje je, ali lahko inovatorju ponudimo jasno pot do odgovorne uporabe tehnologije namesto regulatornega labirinta. Zato potrebujemo pravila. Vprašanje ni regulacija ali inovacije. Pravo vprašanje je, kakšna regulacija omogoča odgovorne inovacije. Če umetna inteligenca odloča o tem, ali bo posameznik dobil zaposlitev, kredit

Foto: Unsplash

ali dostop do pomembne storitve, je razumljivo, da zahtevamo visoko raven preglednosti in nadzora. Če pa podjetje uporablja umetno inteligenco za urejanje dokumentov ali pripravo povzetka sestanka, potrebujemo drugačen pristop. Ni vsak algoritem grožnja človeštvu. Nekateri nam samo pomagajo najti dokument, ki smo ga pred tremi meseci shranili pod imenom »končna_verzija_res_zadnja_FINAL_7.docx«.

Konkurenčnost Evrope

V ozadju razprave o digitalnem omnibusu pa je še večje vprašanje: konkurenčnost Evrope. Svet se ne ustavlja. Združene države imajo izjemno sposobnost, da inovacije hitro spremenijo v globalna podjetja. Kitajska z velikimi strateškimi vlaganji razvija svoje tehnološke zmogljivosti. Evropa pa mora najti svojo pot. Digitalni omnibus je zato priložnost, da Evropa pokaže zrelost. Da prizna, da lahko tudi dober sistem postane boljši. Potrebujemo pravila, ki varujejo ljudi, vendar ne prestrašijo inovatorjev. Pravila, ki preprečujejo zlorabe, vendar omogočajo razvoj. Pravila, ki podjetjem pokažejo pot naprej, namesto da jim ponudijo zemljevid s preveč različnimi legendami.

Kibernetska varnost je postala preizkus odpornosti

Kibernetsko varnost smo dolgo opisovali z jezikom obrambnih zidov. A danes to ni dovolj.

Omrežje je bilo grad, požarni zid so bila vrata, uporabniki so bili nekje znotraj, napadalci pa zunaj. Takšna slika je bila priročna, nikoli pa posebej natančna. Danes je že skoraj neuporabna. Podjetje nima več enega roba. Ima oblak, oddaljene uporabnike, zunanje izvajalce, mobilne naprave, SaaS aplikacije, integracije, razvojna okolja, API-je, pametne naprave, varnostne kopije, domenske račune in stare sisteme, ki jih nihče ne želi izklopiti, ker še vedno nekako delujejo.

Kibernetska varnost je zato postala manj podobna zaklepanju vrat in bolj podobna stalnemu upravljanju tveganja. Podjetja se ne sprašujejo več, ali bodo napadena, bolj pomembno je postalo, kako hitro bodo napad prepoznala, koliko škode bodo omejila in ali bodo po incidentu lahko nadaljevala z delom.

Napadi so hitrejši, manj hrupni in bolj poslovno naravnani. Napadalci ne iščejo več samo strežnika, ki ga lahko okužijo z zlonamerno programsko opremo. Iščejo dostop, podatke, žetone, administrativne račune, nepopravljene robne naprave, slabo nadzorovane integracije in procese, pri katerih lahko organizacijo stisnejo tam, kjer najbolj boli. Včasih je to proizvodnja. Včasih bolnišnični sistem. Včasih računovodstvo. Včasih pa zadošča že grožnja, da bodo javno objavili podatke kupcev.

Ranljivosti so postale vhodna vrata, ne tehnična opomba

Dolgo je veljalo, da so ukradena gesla najpogostejša pot v sistem. To še vedno ostaja veliko tveganje, vendar se razmerje spreminja. Izkoriščanje ranljivosti programske opreme, naprav in spletnih storitev je postalo ena glavnih začetnih točk napadov. Razlog je preprost. Svet je preveč povezan in prepočasen pri krpanju ranljivosti.

Ranljivost je točka, kjer se predpostavke razvijalca, konfiguracija sistema in dejansko vedenje napadalca srečajo na najneprijetnejši možen način. Če je ranljivost v javno dostopni storitvi, na primer v VPN prehodu, požarnem zidu, sistemu za oddaljeni dostop ali spletnem vmesniku, napadalec pogosto ne potrebuje uporabnika, ki klikne na napačno povezavo. Dovolj je avtomatizirano iskanje ranljivih sistemov.

Zato je upravljanje ranljivosti postalo ena najpomembnejših disciplin v varnosti. Ne gre samo za nameščanje popravkov. Najprej je treba vedeti, kaj organizacija sploh ima. Nato mora vedeti, kateri sistemi so izpostavljeni internetu, kdo je odgovoren zanje, kako hitro jih je mogoče posodobiti in kaj se zgodi, če popravka ni mogoče namestiti takoj. Veliko podjetij pri tem pade pri osnovnem vprašanju – inventarju. Ne morejo zaščititi sistema, za katerega ne vedo, da obstaja. Dovolj je lahko že pozabljen testni strežnik, star VPN, neuporabljen uporabniški račun ali omrežna naprava brez centralnega beleženja. Napadalec ne išče najbolj pomembnega sistema. Išče najlažji vhod, nato pa se premakne naprej.

Tiha tarča so postale omrežne robne naprave

Varnostni oddelki so veliko let nadzor gradili okoli računalnikov in strežnikov. Na njih tečejo EDR rešitve, beležijo se procesi, spremljajo se datoteke, zaznava se nenavadno vedenje. Napadalci so to opazili. Zato se vse pogosteje selijo na naprave, ki stojijo med omrežji: VPN prehode, usmerjevalnike, požarne zidove, naprave za uravnoteženje prometa in virtualizacijsko infrastrukturo. Te naprave so mamljive iz več razlogov. Pogosto so neposredno izpostavljene internetu. Pogosto imajo visoko stopnjo dovoljenj v

omrežju. Pogosto jih ni mogoče nadzorovati z istimi orodji kot navadne računalnike. In pogosto se jih ne posodablja tako hitro, kot bi se jih moralo, ker so kritične za delovanje podjetja. Nihče si ne želi sredi delovnega dne ponovno zagnati VPN prehoda, ki ga uporablja celotna prodajna ekipa. Napadalci na takšnih napravah pogosto ne potrebujejo klasične zlonamerne programske opreme. Uporabijo lahko vgrajene funkcije, administrativne ukaze, zajem prometa ali začasno kodo v pomnilniku. Tak napad je težje opaziti, ker za seboj ne pusti običajnih sledi na delovni postaji.

Za podjetja to pomeni, da je centralno beleženje bolj kot ne nujna izbira. Zapisi omrežnih naprav, administrativni dostopi, spremembe konfiguracij, poskusi prijave in vzorci prometa morajo biti shranjeni dovolj dolgo, da imajo preiskovalci po incidentu sploh kaj analizirati. Če naprava hrani zapise samo nekaj dni, napadalec pa je v omrežju več tednov, je preiskava že na začetku na mrtvi točki.

Ransomware ni več samo šifriranje datotek

Ransomware je v javnosti še vedno razumljen kot napad, pri katerem se datoteke zaklenejo, podjetje pa dobi zahtevo za odkupnino. To je samo en del zgodbe. Sodobne izsiljevalske skupine pogosto najprej ukradejo podatke, šele nato šifrirajo sisteme. Če žrtev obnovi podatke iz varnostnih kopij, ostane grožnja, da bodo napadalci javno objavili dokumente, pogodbe, osebne podatke, poslovne skrivnosti …

Varnostne kopije so nujne, vendar same po sebi niso več dovolj. Če organizacija lahko obnovi strežnike, ne more pa preprečiti objave ukradenih podatkov, ima še vedno resen incident.

Napadalci pri tem pogosto razumejo poslovanje žrtve bolje, kot bi si podjetje želelo. Vedo, kateri sistemi so kritični. Vedo, kdaj je pritisk največji. Vedo, da javna objava podatkov kupcev ali pacientov ni samo tehnična težava, ampak lahko pomeni komunikacijsko, pravno in finančno krizo.

Zato obramba pred ransomware napadi ne sme biti omejena na protivirusni program. Potrebuje segmentacijo omrežja, omejevanje privilegijev, varnostne kopije brez možnosti enostavnega brisanja, preizkušene postopke obnove in jasen načrt komuniciranja.

Identiteta je nova infrastruktura

Danes je uporabniški račun pogosto pomembnejši od naprave. Če napadalec dobi veljavne prijavne podatke, se lahko obnaša kot uporabnik. Če dobi administratorski račun, lahko obide številne tehnične kontrole. Če dobi sejne piškotke ali OAuth žetone, lahko včasih dostopa do aplikacij, ne da bi ponovno sprožil večfaktorsko avtentikacijo.

To je razlog, da se varnost premika od gesel k močnejšim načinom prijave. Klasična večfaktorska avtentikacija (MFA) je še vedno veliko boljša kot samo geslo, vendar niso vsi MFA načini enako odporni. SMS kode, potisna obvestila in enkratne kode lahko napadalci v določenih scenarijih prestrežejo, izsilijo ali uporabnika prepričajo, da jih vnese na lažno stran.

Passkey prijave in FIDO2 varnostni ključi so pomembni zato, ker temeljijo na kriptografiji javnega ključa. Uporabnik ne vnaša skrivnosti, ki bi jo lahko napadalec preprosto prepisal. Zasebni ključ ostane na napravi, storitev pa preveri, ali se uporabnik res prijavlja na pravo domeno. To phishing napade močno oteži, ker lažna stran ne more enostavno ponovno uporabiti ukradenega gesla ali kode.

Za podjetja to ne pomeni, da morajo jutri izbrisati vsa gesla. Pomeni pa, da morajo najprej zaščititi najbolj občutljive račune.

UI je pospeševalnik, ne samostojen napadalec

Umetna inteligenca je v kibernetski varnosti pogosto predstavljena dramatično, včasih skoraj filmsko. Bolj trezna slika je manj spektakularna, a resnejša. UI napadalcem za zdaj najpogosteje pomaga pri hitrosti, obsegu in kakovosti izvedbe. Phishing sporočila so bolj tekoča. Prevajanje v lokalne jezike je boljše. Lažne prijave za delo, sporočila podpore, prevare z računi in imitacije internih sporočil so prepričljivejše. Napadalec z manj znanja lahko hitreje pripravi boljši napad.

To ne pomeni, da je vsako phishing sporočilo zdaj genialno. Je pa dejstvo, da stari signali, na katere so se uporabniki zanašali, izgubljajo vrednost. Včasih je bila zanesljiv znak prevare slaba slovnica, danes so sporočila precej prepričljiva. Enako velja za ton sporočila. Generativna orodja lahko ustvarijo besedila, ki zvenijo dovolj poslovno, lokalno in nujno. Moramo pa se zavedati, da je prav človek eden bolj pomembnih in ranljivih členov v varnostni verigi. En klik lahko napadalcu na široko odpre vrata v sistem kljub vsem ostalim varnostnim ukrepom. UI pa se uporablja tudi v obrambi. Pomaga pri razvrščanju opozoril, povzemanju incidentov, iskanju vzorcev in avtomatizaciji dela varnostnih analitikov. A tudi tu velja previdnost. Model, ki samozavestno povzame napačne podatke, lahko naredi veliko škodo. Varnostna ekipa ne potrebuje samo hitrega, ampak preverljiv odgovor. Zato bo vloga UI v varnosti najverjetneje hibridna: stroj bo pospešil analizo, človek pa bo moral razumeti posledice odločitve.

Največje tveganje pri UI v podjetjih ni vedno napad od zunaj. Pogosto je nenadzorovana uporaba od znotraj. Zaposleni v javna orodja kopirajo izvorno kodo, pogodbe, osebne podatke, finančne tabele ali interne dokumente, ker želijo hitrejši povzetek ali boljše besedilo.

Napad na enega, posledice za mnoge

Programska oprema je sestavljena iz plasti. Aplikacija uporablja knjižnice, te uporabljajo druge knjižnice, infrastruktura uporablja zabojnike, razvoj poteka prek repozitorijev, gradnja prek CI/CD sistemov, produkcija pa pogosto temelji na storitvah zunanjih ponudnikov. Napad na dobavno verigo izkorišča prav to povezanost.

Klasičen primer je ranljiva knjižnica, ki jo uporablja veliko projektov. Drugi primer je zlorabljena posodobitev programske opreme. Tretji je ukraden dostop do razvojnega okolja. Četrti je zlonameren paket v javnem repozitoriju, ki ima ime skoraj enako kot legitimna knjižnica. V vseh primerih napadalec ne napada nujno končnega podjetja neposredno. Napade nekaj, čemur podjetje zaupa.

Zato postajajo SBOM dokumenti pomembnejši. SBOM je seznam sestavnih delov programske opreme, nekakšen inventar knjižnic, komponent in odvisnosti. Sam po sebi ne prepreči napada. Pomaga pa odgovoriti na vprašanje, ki se pojavi po objavi nove kritične ranljivosti. Ali je prizadeta komponenta sploh v uporabi in kje?

Kibernetska varnost je zrelostni test

Največja razlika med zrelo in nezrelo organizacijo ni v tem, da prva nikoli nima incidenta. Razlika je v tem, da zna prva incident omejiti. Ve, kaj ima, kdo odloča, kateri sistemi imajo prednost. Ve, kje so dokazi, kako obnoviti podatke, koga obvestiti, kaj lahko izklopi brez ogrožanja poslovanja.

Napadi bodo vse hitrejši. UI bo povečala obseg socialnega in tehničnega pritiska. Ransomware se bo še naprej prilagajal. Napadi na dobavno verigo in SaaS integracije bodo ostali privlačni, ker omogočajo velik doseg. Robne naprave bodo ostale problem, dokler jih podjetja ne bodo začela obravnavati kot kritične sisteme.

Dobra novica je, da obramba ni brez moči. Organizacije poznajo večino ukrepov, ki zmanjšajo tveganje. Težava je izvajanje. Varnost pogosto ne odpove zato, ker ni bilo znanja, ampak ker ni bilo discipline, lastništva in časa.

DIGITALNA SUVERENOST

Made in EU: konkurenčna prednost sodobne kibernetske varnosti

Evropsko poreklo kibernetskih rešitev danes pomeni bistveno več kot geografski izvor. Organizacijam prinaša več zaupanja, manj poslovnih tveganj ter večjo digitalno suverenost.

V času zaostrenih geopolitičnih razmer, vse agresivnejših kibernetskih napadov in vse strožje evropske regulative postaja oznaka Made in EU pomemben kriterij pri izbiri rešitev za informacijsko in kibernetsko varnost. Ne gre več zgolj za vprašanje tehnološke odličnosti, temveč tudi zaupanja. Rešitve, razvite v Evropski uniji, nastajajo pod evropsko zakonodajo, spoštujejo visoke standarde varstva podatkov in transparentnosti razvoja ter organizacijam omogočajo lažje izpolnjevanje zahtev direktive NIS2, uredb GDPR in DORA. Hkrati zmanjšujejo tveganja, povezana z dobavno verigo programske opreme, na primer problem stranskih vrat, in tveganja, povezana z odvisnostjo od tehnologij, ki nastajajo zunaj evropskega pravnega prostora.

Rešitve iz EU kot odgovor na nova poslovna tveganja

Kljub jasnim zahtevam pa evropski izvor sam po sebi ni dovolj. Organizacijam mora takšna rešitev prinesti tudi merljivo zmanjšanje poslovnih tveganj in najmanj primerljivo raven kibernetske varnosti in odpornosti.

Prvo med njimi je tveganje uspešnega kibernetskega napada. ESET že več kot 35 let razvija lasten tehnološki sklad za zaščito končnih točk, omrežij, elektronske pošte in oblačnih storitev ter napredno zaznavanje groženj. Ko organizacija potrebuje še višjo raven zaščite, tehnologijo dopolnijo tovarniške storitve ESET MDR (Managed Detection and Response). Te na podlagi globalnega varnostnega obveščanja, umetne inteligence in strokovnjakov ESET-ovega lastnega evropskega varnostno-operativnega centra zagotavljajo neprekinjeno spremljanje okolja, zgodnje odkrivanje napadov in hitro odzivanje na incidente. Tako podjetje bistveno skrajša čas, v katerem lahko napadalec povzroča poslovno škodo in posledično minimizira potencialno škodo.

ESET ima posebno mesto med evropskimi proizvajalci tudi zaradi dolgoletnih vlaganj v umetno inteligenco. Letos je podjetje napovedalo 40-milijonsko naložbo v razvoj umetne inteligence, povezane z zagotavljanjem kibernetske varnosti. Z razvojem lastnih modelov umetne inteligence, nadaljnjim razvojem storitev MDR ter zaposlitvijo približno tisoč novih raziskovalcev in razvojnih inženirjev pomembno krepi evropsko tehnološko neodvisnost in dokazuje, da Evropa ni zgolj regulator digitalnega prostora, temveč tudi eden njegovih pomembnih inovatorjev.

Drugo pomembno področje predstavlja zaščita poslovnih informacij. Safetica DLP organizacijam omogoča nadzor nad uporabo občutljivih podatkov, preprečuje njihovo nenamerno ali namerno razkritje ter pomaga dokazovati skladnost z zakonodajo in internimi pravili. V času, ko podatki

predstavljajo eno najpomembnejših poslovnih sredstev, takšna zaščita pomembno zmanjšuje operativna in poslovna tveganja ter ohranja vrednost premoženja, ki se nahaja v znanju.

Enako pomemben je nadzor nad privilegiranimi dostopi. Napadalci po uspešnem vdoru praviloma poskušajo pridobiti administratorske pravice, zato Excalibur PAM z upravljanjem privilegiranih računov, nadzorom administrativnih sej, večfaktorsko avtentikacijo in načelom najmanjših privilegijev učinkovito omejuje možnost zlorab ter preprečuje širjenje napadalcev po informacijskem okolju.

Evropske tehnologije, podprte z lokalnim znanjem

Slovenska podjetja imajo pri tem še dodatno prednost. Evropske rešitve ESET, Safetica in Excalibur so jim na voljo skupaj z lokalno strokovno podporo podjetja Si Splet, ki zagotavlja svetovanje, implementacijo ter tehnično pomoč v slovenskem jeziku. Tako organizacije združijo prednosti evropskih tehnologij z lokalnim znanjem in hitrim odzivom, kar je pri obvladovanju kibernetskih incidentov pogosto odločilnega pomena.

Na trgu se že pozna, da organizacije kibernetske rešitve vse manj izbirajo glede na število funkcionalnosti. Enako pomembno bo, kdo jih razvija, pod katero zakonodajo nastajajo in kako učinkovito zmanjšujejo poslovna tveganja. Za slovenske organizacije zato Made in EU ne pomeni zgolj izbire evropske tehnologije. Pomeni izbiro rešitev, ki temeljijo na evropskem znanju, zakonodaji in vrednotah ter lokalni podpori, kar doprinaša kakovostnejšo uporabniško izkušnjo ter varnostni sistem, ki podpira vse vidike tveganj, od vrhunske zaščite do zagotavljanja skladnosti. (P.R.)

Kaj organizacija pridobi s predstavljenimi EU-kibernetskimi rešitvami?

- Proaktivno zaščito in manjše tveganje uspešnega kibernetskega napada.
- Hitrejše odkrivanje in odzivanje na incidente 24/7 z globalnim varnostnim obveščanjem in tovarniško ekipo strokovnjakov.
- Zaščito občutljivih poslovnih podatkov.
- Nadzor nad privilegiranimi dostopi ter uporabniškimi kompetencami.
- Lažje izpolnjevanje zahtev NIS2, GDPR in DORA.
- Večjo digitalno suverenost in manjšo odvisnost od tehnologij zunaj EU.
- Lokalno strokovno podporo in svetovanje v slovenskem jeziku.

NOVA RAVEN UPRAVLJANJA PODATKOV

Sodobni podatkovni center v Ljubljani

Prenovljen podatkovni center v lasti podjetja Informatika d.o.o. združuje vrhunsko varnost, napredno signalizacijo, inteligentno upravljanje in popoln pregled nad povezavami – s pripravljenostjo na AI in prihodnjo rast.

Zanesljivo upravljanje podatkov postaja ključna konkurenčna prednost podjetij. Podatkovni center v Ljubljani, ki je v lasti podjetja Informatika d.o.o., predstavlja sodoben pristop k upravljanju infrastrukture, kjer so v ospredju varnost, preglednost in popoln nadzor nad sistemom.

Celovito integriran nadzorni sistem

Prenovljeni podatkovni center združuje vrhunsko tehnološko infrastrukturo in napredne pristope upravljanja. Posebnost predstavlja celovito integriran nadzorni sistem, ki omogoča natančen vpogled v delovanje, hkrati pa z napredno signalizacijo zagotavlja takojšnjo vizualno povratno informacijo neposredno na nivoju posameznih omar. Tak pristop omogoča izjemno hitro zaznavanje stanja in bistveno skrajša odzivne čase.

Pomembna prednost centra je tudi lastna rešitev za popis in dokumentacijo povezav. Sistem omogoča popolno sledljivost – v vsakem trenutku je jasno, katera povezava je aktivna, kakšen je njen namen ter kako je vzpostavljena. Takšna transparentnost bistveno zmanjšuje možnost napak ter omogoča učinkovitejše upravljanje tudi v kompleksnih IT okoljih.

Učinkovito upravljanje energije in zanesljivo delovanje

Podatkovni center vključuje sodobne sisteme za upravljanje napajanja in energije, ki omogočajo natančno spremljanje porabe in optimizacijo delovanja. V kombinaciji z učinkovitim hlajenjem infrastruktura zagotavlja stabilno okolje tudi pri večjih obremenitvah.

Velik poudarek je namenjen tudi varnosti, kjer se prepletajo fizična zaščita, nadzor dostopa in napredni nadzorni sistemi. Takšna zasnova zagotavlja visoko stopnjo zaščite in zanesljivo delovanje kritične infrastrukture.

Modularen sistem, ki je pripravljen na prihodnost

Posebna vrednost podatkovnega centra je njegova modularna zasnova, ki omogoča enostavno širitev, prilagoditve in integracijo novih tehnologij brez zapletov. Infrastruktura je pripravljena na prihodnje potrebe, vključno z zahtevnimi okolji, kot so umetna inteligenca (AI), analitika velikih podatkov in druge sodobne IT rešitve. Center obenem razpolaga z zadostnimi prostimi kapacitetami, kar omogoča hitro vključevanje novih uporabnikov ali širitev obstoječih sistemov brez dodatnih infrastrukturnih posegov.

Uspešno izveden projekt prenove

Projekt prenove je potekal pod okriljem podjetja Informatika d.o.o., ki ga vodi direktor mag. Jože Knavs, tehnično izvedbo in koordinacijo pa je vodil Rok Berdajs. Končni rezultat predstavlja sodoben podatkovni center, ki združuje visoko razpoložljivost, napredno upravljanje in popoln nadzor nad infrastrukturo.

Prenovljeni podatkovni center v Ljubljani tako postavlja standard sodobne IT infrastrukture – kot okolje, ki ni le stabilno in varno, temveč tudi pripravljeno na prihodnost. Več lahko najdete na spletni strani www.informatika.si. (P.R.)

Informacijske storitve in inženiring, d.o.o.
INFORMATIKA

INFORMATIKA d. o. o.
Vetrinjska ulica 2
2000 Maribor

T: +386 2 707 10 00
info@informatika.si
www.informatika.si

ANNI D.O.O.

Ne ugibajte, preverite: kako zanesljiva je vaša digitalna zaščita?

Digitalno okolje je danes srce vsake organizacije.

Poslovni procesi, komunikacija, dokumentacija in ključni podatki so odvisni od informacijskih sistemov, zato kibernetska varnost že dolgo ni več zgolj tehnično vprašanje, ampak pomemben del poslovne strategije.

Kibernetski napadi postajajo vse bolj ciljani, avtomatizirani in poslovno motivirani. Ob tem niso ogrožena le velika podjetja – vse pogosteje so tarča tudi mala in srednje velika podjetja ter javne ustanove. Hkrati zakonodaja, kot so NIS2, ZInfV-1 in GDPR, od organizacij zahteva sistematično upravljanje tveganj ter dokazljivo izvajanje varnostnih ukrepov.

Vsaka organizacija je lahko tarča

Napadalci danes ne iščejo le tehničnih ranljivosti. Izkoriščajo tudi neustrezne nastavitve, zastarele sisteme, pomanjkljive procese in človeške napake.

Posledice so lahko resne:

- prekinitev poslovanja,
- izguba ali zloraba podatkov,
- finančna škoda,
- izguba zaupanja strank in partnerjev,
- regulatorne in pravne posledice.

Vprašanje zato ni več, ali je organizacija zanimiva za napadalce, ampak ali je nanje dovolj pripravljena.

Tveganja niso vedno vidna

Veliko ranljivosti ostane skritih, dokler ne pride do varnostnega incidenta. Informacijski sistemi lahko delujejo brezhibno, v ozadju pa obstajajo nepravilne konfiguracije, zastarela programska oprema ali neustrezno upravljani dostopi.

Zato je redno preverjanje stanja varnosti eden najučinkovitejših preventivnih ukrepov.

Varnostni pregled IKT okolja pokaže dejansko stanje

Pri kibernetski varnosti velja preprosto pravilo – **ne ugibajte, preverite**.

Varnostni pregled IKT okolja organizaciji omogoča objektiven vpogled v trenutno stanje zaščite. Pregled vključuje analizo infrastrukture, konfiguracij, uporabniških dostopov ter iskanje morebitnih ranljivosti in odstopanj od dobrih praks.

Na podlagi ugotovitev organizacija prejme jasna priporočila za izboljšave, razvrščena glede na stopnjo tveganja in vpliv na poslovanje.

Takšen pregled je primerljiv s tehničnim pregledom avtomobila – morebitne težave odkrije pravočasno, še preden povzročijo večjo škodo ter ogrozijo poslovne procese.

Učinkovita zaščita temelji na tehnologiji in ljudeh

Tudi najboljše tehnične rešitve niso dovolj, če zaposleni ne prepoznajo sodobnih kibernetskih groženj. Človek ostaja ena najpogostejših vstopnih točk za napadalce, zato sta ozaveščanje in redno izobraževanje pomemben del celovite varnostne strategije. Šele kombinacija ustrezno zaščitene infrastrukture, dobro postavljenih procesov in ozaveščenih zaposlenih zagotavlja visoko stopnjo odpornosti organizacije.

Kibernetska varnost je naložba v zanesljivo poslovanje

V podjetju **Anni – Center za kibernetsko varnost** organizacijam pomagajo pridobiti jasen vpogled v dejansko stanje njihove digitalne zaščite. Z varnostnim pregledom IKT okolja prepoznajo ključna tveganja, pripravijo konkretna priporočila za izboljšave in pomagajo pri njihovem odpravljanju. Kibernetska varnost ni enkraten projekt, ampak neprekinjen proces. Organizacije, ki svoje digitalno okolje redno preverjajo in izboljšujejo, so bolje pripravljene na sodobne grožnje, lažje izpolnjujejo regulatorne zahteve in zagotavljajo varno ter zanesljivo poslovanje.

Več informacij: www.varen.it. (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

INTERVJU: dr. Niko Gamulin, vršilec dolžnosti direktorja URSIV

»Napadalci ne izbirajo žrtev po velikosti, temveč po ranljivosti«

O aktualnem stanju kibernetske varnosti, izzivih ob uvedbi NIS2 in vlogi umetne inteligence smo se pogovarjali z dr. Nikom Gamulinom, novim vršilcem dolžnosti direktorja URSIV.

Kako ocenjujete trenutno stanje kibernetske varnosti v Sloveniji in kateri so največji izzivi, s katerimi se soočajo organizacije?

URSIV je nacionalni organ za informacijsko varnost, ki povezuje ključne deležnike, nudi strokovno podporo zavezancem, koordinira preventivne aktivnosti ter skrbi za mednarodno sodelovanje in obvladovanje kibernetskih incidentov ter kriz. Znotraj URSIV deluje tudi inšpekcija za informacijsko varnost. Na podlagi razpoložljivih podatkov ocenjujemo, da je stopnja kibernetske ogroženosti v Sloveniji srednja. Slovenija je v zadnjih letih pomembno okrepila nacionalni sistem kibernetske varnosti. Sprejem Zakona o informacijski varnosti (ZInfV-1) predstavlja pomemben korak k večji odpornosti države, gospodarstva in javnega sektorja.

Organizacije se soočajo z različnimi izzivi. Zlasti javni sektor je še v fazi dviga zrelosti in je pogosto tarča napadov oziroma poskusov zlorab. Opažamo pomanjkljive analize tveganj, neustrezno ali premalo operativno varnostno dokumentacijo, premalo usposabljanj zaposlenih, nepreizkušene načrte odzivanja na incidente ter premalo sistematično upravljanje dobaviteljev, dostopov in varnostnih kopij. Pri ZInfV-1 ni dovolj, da so ukrepi zapisani; biti morajo uvedeni, sorazmerni, preverljivi in redno preizkušeni v praksi.

Kje so največji izzivi pri uvajanju NIS2 in na kaj bi se morale osredotočiti organizacije?

NIS2 od organizacij zahteva, da na podlagi ocene tveganj vzpostavijo in izvajajo postopke za obvladovanje incidentov, pripravijo načrte neprekinjenega poslovanja in redno usposabljajo zaposlene. V praksi to pomeni tudi samoregistracijo zavezancev, določitev odgovornih in kontaktnih oseb, pravilno razvrstitev storitev in sistemov, urejene priglasitve pomembnih incidentov pristojnim skupinam CSIRT ter dokazljivo izvajanje varnostnih ukrepov.

Posebej pomembna je vloga vodstva. ZInfV-1 jasno določa odgovornost vodstvenih oziroma odgovornih oseb za upravljanje informacijske in kibernetske varnosti. Ta odgovornost ne sme ostati zgolj pri IT-oddelku: vodstvo mora poznati ključna tveganja, zagotoviti vire, potrjevati varnostne politike, spremljati izvajanje ukrepov in zahtevati redno poročanje o incidentih, vajah ter odpravi ugotovljenih pomanjkljivosti.

Ali mala in srednja podjetja res niso zanimiva tarča za kibernetske napadalce?

Napadalci ne izbirajo žrtev po velikosti, temveč po ranljivosti, zato so mala in srednja podjetja pogosto privlačna tarča. Poleg neposrednih posledic lahko predstavljajo tudi vstopno točko za napade na večje organizacije in druge partnerje v dobavni verigi. Manjše organizacije lahko z relativno preprostimi ukrepi bistveno zmanjšajo tveganja: večfaktorsko avtentikacijo, rednim posodabljanjem, varnostnimi kopijami, jasnimi pravili uporabe službenih naprav, usposabljanjem zaposlenih in osnovnim načrtom odziva na incident.

Kako umetna inteligenca spreminja področje kibernetske varnosti?

Umetna inteligenca je postala vprašanje gospodarske in tehnološke suverenosti. Evropa išče ravnotežje med varnostjo, regulacijo in konkurenčnostjo, Slovenija pa mora vlagati predvsem v znanje, razvoj kompetenc in odgovorno uporabo umetne inteligence.

Zato morajo organizacije poleg priložnosti obravnavati tudi tveganja: zlorabo zaupnih ali osebnih podatkov, odvisnost od zunanjih ponudnikov, nepojasnjene odločitve modelov, manipulacijo vhodnih podatkov in potrebo po človeškem nadzoru nad rezultati.

Pri uvajanju umetne inteligence je treba določiti jasna pravila glede podatkov, dostopov, sledljivosti, odgovornosti in preverjanja rezultatov. Za organizacije, zlasti za zavezance po ZInfV-1, mora biti uporaba umetne inteligence del obvladovanja tveganj. Zmogljivosti umetne inteligence se vse bolj uveljavljajo kot strateška infrastruktura dvojne rabe, pomembna za gospodarstvo, varnost, obrambo in javni sektor.

Katere aktivnosti oziroma projekti bodo v prihodnjem obdobju v ospredju vašega dela?

Med prednostnimi nalogami ostajajo podpora zavezancem pri izvajanju ZInfV-1, krepitev kibernetske odpornosti, ozaveščanje javnosti, usposabljanje organizacij in izboljšanje procesov prijavljanja ter obravnave incidentov. Konkretno to pomeni nadaljnjo strokovno in metodološko podporo zavezancem, pripravo in posodabljanje smernic, vzorčne dokumentacije in orodij za samooceno, krepitev sistema priglašanja incidentov, usposabljanja odgovornih oseb, vaje, preventivne aktivnosti ter sodelovanje v evropskih in mednarodnih mehanizmih kibernetske varnosti, vključno z nalogami NCC-SI in sodelovanjem pri obvladovanju kibernetskih kriz. Krepili bomo mednarodno sodelovanje in pripravljenost na nove tehnološke izzive.

dr. Niko Gamulin (Foto: Danijel Novaković, STA)

Kaj bi svetovali direktorjem in vodjem IT na področju informacijske varnosti?

Vodstvom bi svetoval, da informacijsko varnost obravnavajo kot del strateškega upravljanja tveganj in kot naložbo v poslovno odpornost. Največjo razliko še vedno naredijo ljudje, ki so dobro usposobljeni. Začeti je treba z osnovnimi vprašanji: katere storitve moramo ohraniti tudi v kriznih razmerah, kateri podatki so kritični, kdo ima administratorske dostope, od katerih dobaviteljev smo odvisni, in kako hitro lahko po incidentu ponovno vzpostavimo delovanje. Varnost mora biti vključena tudi v pogodbe z dobavitelji, poslovne načrte, investicije, usposabljanja in redno poročanje vodstvu. (P.R.)

vCISO

Vse več podjetij ima virtualnega CISO-ja. Razlog ni le zakonodaja

Vodenje kibernetske varnosti je v zadnjih letih postalo pomemben del poslovnega upravljanja. Če je bilo nekoč mogoče odgovornost prepustiti predvsem oddelku IT, danes to ne velja več.

Zakonodaja od vodstva podjetij zahteva aktivno upravljanje tveganj, ob morebitnem varnostnem incidentu pa se presoja predvsem, ali je podjetje ravnalo skrbno in sprejemalo utemeljene odločitve.

To pomeni, da direktorji ne odgovarjajo več le za poslovne rezultate, temveč tudi za ustrezno upravljanje informacijske varnosti. Ker zaposlitev lastnega strokovnjaka za številna srednje velika podjetja predstavlja velik organizacijski in finančni zalogaj, se vse več organizacij odloča za virtualnega CISO-ja oziroma storitev vCISO.

> Večina srednje velikih podjetij ne potrebuje CISO-ja za polni delovni čas, potrebuje pa nekoga, ki zna tveganja prepoznati, jih predstaviti vodstvu v razumljivem jeziku ter podjetje usmerjati pri izpolnjevanju zakonskih obveznosti in učinkovito komunicirati z regulatorji.

Nova realnost za vodstva podjetij

Odgovornost za kibernetsko varnost danes sega precej dlje od izbire tehničnih rešitev. Če pride do incidenta, je seveda pomembno vprašanje, ali je podjetje uporabljalo ustrezno zaščito, še bolj pa, ali je vodstvo poznalo tveganja, sprejelo ustrezne ukrepe in lahko svoje odločitve tudi utemelji.

Prav zato številna podjetja iščejo strokovnjaka, ki pomaga pri sprejemanju odločitev, pripravi varnostnih politik, ocenjevanju tveganj in komunikaciji z regulatorji. To vlogo prevzame virtualni CISO, ki podjetju zagotavlja strokovno podporo brez potrebe po zaposlitvi lastnega vodje informacijske varnosti.

Zakaj zanimanje tako hitro narašča?

V Telemachu Slovenija opažajo izrazito rast zanimanja za storitev vCISO. Povpraševanje je naraslo do te mere, da se že pojavljajo izzivi z razpoložljivostjo terminov.

Dejan Trop, svetovalec za kibernetsko varnost pri Telemachu pojasnjuje, da podjetja, ki so pred letom ali dvema še razmišljala, ali sploh sodijo med zavezance po Zakonu o informacijski varnosti (ZInfV-1), danes to že vedo. Zdaj jih zanima predvsem, kako bodo zahteve zakona tudi dejansko izpolnila.

Gre za pomembno spremembo v razmišljanju vodstev. Kibernetska varnost ni več področje, s katerim se podjetje ukvarja šele po incidentu, ampak postaja del vsakodnevnega upravljanja poslovnih tveganj.

vCISO je več kot le zunanji IT-svetovalec

Storitev vCISO pogosto napačno razumemo kot občasno svetovanje zunanjega IT-strokovnjaka. V resnici gre za celovito funkcijo. Virtualni CISO sodeluje pri upravljanju informacijskih tveganj, pripravlja varnostne politike, pomaga pri izpolnjevanju regulatornih zahtev in vodstvu svetuje pri sprejemanju ključnih odločitev.

Podjetje tako pridobi izkušenega strokovnjaka, ki razume tako tehnični kot poslovni vidik kibernetske varnosti. Njegova naloga ni le opozarjanje na pomanjkljivosti, ampak predvsem pomoč pri oblikovanju procesov, ki zmanjšujejo tveganja in povečujejo odpornost organizacije.

Kot poudarja Trop, večina srednje velikih podjetij ne potrebuje CISO-ja za polni delovni čas, potrebuje pa nekoga, ki zna tveganja prepoznati, jih predstaviti vodstvu v razumljivem jeziku ter podjetje usmerjati pri izpolnjevanju zakonskih obveznosti in učinkovito komunicirati z regulatorji.

Pregled stanja, načrt, ukrepi

Sodelovanje se začne s pregledom obstoječega stanja. Virtualni CISO analizira informacijsko infrastrukturo, oceni tveganja in skupaj z vodstvom določi ključna področja, ki jih je treba zaščititi. Pri tem ne gre zgolj za tehnologijo, ampak predvsem za razumevanje poslovnih procesov.

Na podlagi analize pripravi načrt aktivnosti, nato pa spremlja izvajanje ukrepov, sodeluje na sestankih vodstva, pomaga pri posodabljanju varnostnih politik ter svetuje ob spremembah zakonodaje ali poslovnega okolja.

Pomembna je tudi njegova vloga ob varnostnem incidentu. Vodstvo mora takrat hitro dobiti odgovore na vprašanja, kaj se je zgodilo, kakšne so posledice in kateri bodo naslednji koraki. Takšnih odločitev ni mogoče sprejemati na podlagi ugibanj, temveč na podlagi vnaprej pripravljenih postopkov in jasno določenih odgovornosti.

vCISO je pogosto najboljša odločitev

Za številna srednje velika podjetja je zaposlitev lastnega vodje informacijske varnosti težko izvedljiva. Model vCISO omogoča hitrejšo vzpostavitev ustreznega upravljanja informacijske varnosti, dostop do širšega nabora strokovnega znanja ter večjo prilagodljivost, hkrati pa podjetje ohrani nadzor nad stroški.

Časa za odlašanje je vse manj

Pomemben razlog za že omenjeno povečano zanimanje za storitev vCISO ostaja tudi Zakon o informacijski varnosti (ZInfV-1), ki je jasno opredelil odgovornost poslovodstva za področje kibernetske varnosti. Če se po incidentu izkaže, da vodstvo ni ravnalo z ustrezno skrbnostjo, ima to lahko neposredne posledice za odgovorne osebe.

Vzpostavitev ustreznih procesov zahteva čas, zato odlašanje ni dobra odločitev. Podjetja, ki bodo z uvedbo potrebnih rešitev čakala predolgo, se lahko soočijo z omejeno razpoložljivostjo strokovnjakov in daljšimi čakalnimi roki.

Vprašanje danes zato ni več, ali podjetje potrebuje CISO-ja, temveč ali si lahko še privošči, da te funkcije nima oziroma da njeno vzpostavitev prelaga v prihodnost.

Vprašanje danes zato ni več, ali podjetje potrebuje CISO-ja, temveč ali si lahko še privošči, da te funkcije nima oziroma da njeno vzpostavitev prelaga v prihodnost.

Več lahko najdete na www.telemach.si. (P.R.)

telemach

www.telemach.si

telemach

BUSINESS

Virtualni CISO: strokovna podpora za varnejše poslovanje

Kibernetski napadi niso več vprašanje če, ampak kdaj. Podjetja, ki pravočasno vzpostavijo funkcijo vCISO, hitreje dosežejo skladnost, učinkoviteje upravljajo tveganja in dokazujejo odgovorno ravnanje vodstva.

Zagotovite si izkušenega **strokovnjaka za informacijsko varnost** brez stroškov zaposlitve lastnega CISO.

Glavne prednosti vCISO

Stalno spremljanje skladnosti in izvajanja ukrepov

Mesečno poročanje in maturity pregled

Usklajevanje prioritet z upravo in odgovornimi osebami

Svetovanje pri implementaciji politik in nadzoru tveganj

Podpora pri incidentih, presojah in komunikaciji z zunanjimi deležniki

Priprava letnega poročila o stanju varnosti in skladnosti (za upravo ali regulatorje)

Poskrbite za varnost svojega podjetja že danes.

Kontaktirajte nas na **b2b@telemach.si** in preverite, kako lahko vCISO zaščiti vaše poslovanje.

DATAINFO.SI

Znanje, ki gradi zaupanje v digitalni dobi

Mednarodno certificirana izobraževanja za ISO, GDPR in umetno inteligenco.

Digitalizacija, kibernetska tveganja, umetna inteligenca in strožje zahteve glede skladnosti od organizacij zahtevajo vedno več strokovnega znanja. Informacijska varnost, varstvo osebnih podatkov, upravljanje tveganj in neprekinjeno poslovanje niso več zgolj tehnična ali pravna vprašanja, temveč del odgovornega upravljanja. DATAINFO.SI zato že od leta 2019 sodeluje s PECB, mednarodno priznano organizacijo za certificiranje strokovnjakov na področju standardov ISO, skladnosti in upravljanja. Na to partnerstvo so ponosni, saj jim omogoča, da slovenskim strokovnjakom in organizacijam približajo mednarodno priznana znanja in certificirane programe.

eLearning: prilagodljivo učenje za zaposlene strokovnjake

Ena največjih prednosti PECB eLearning tečajev je fleksibilnost. Udeleženci se lahko učijo kjerkoli in kadarkoli, v svojem tempu. Tak način je primeren za zaposlene strokovnjake, vodje, DPO-je, varnostne strokovnjake, presojevalce, IT osebje in vse, ki težko usklajujejo izobraževanja z delovnimi obveznostmi.

Vsebine so dostopne 24 ur na dan, kar omogoča ponavljanje, poglabljanje znanja in pripravo na izpit. Tečaji vključujejo strokovno gradivo, praktične primere in vaje za razumevanje uporabe standardov v realnem okolju.

Praktična znanja, priprava na certifikat in individualna podpora pred izpitom

PECB tečaji združujejo teorijo in praktično uporabna znanja za vzpostavitev, izvajanje, presojo ali izboljševanje sistemov upravljanja ter obvladovanje tveganj in zahtev standardov.

Po opravljenem usposabljanju in izpitu udeleženec pridobi mednarodno priznani certifikat PECB, ki krepi strokovno kredibilnost posameznika in organizacije.

Pri DATAINFO.SI kandidatom nudijo individualne konzultacije pred izpitom, osebno svetovanje glede izbire tečaja in razlago celotnega procesa. Ker so veliko omenjenih tečajev uspešno zaključili tudi njihovi zaposleni, svetujejo na podlagi lastnih praktičnih izkušenj.

Aktualni certificirani tečaji

V sodelovanju s PECB izvajajo več certificiranih eLearning programov. Na področju neprekinjenega poslovanja so na voljo ISO 22301 Foundation, ISO 22301 Lead Implementer in ISO 22301 Lead Auditor. Namenjeni so vzpostavitvi in presoji sistema upravljanja neprekinjenega poslovanja, ki organizacijam pomaga ohraniti delovanje tudi ob večjih motnjah.

Za upravljanje tveganj sta na voljo ISO 31000 Risk Manager in ISO/IEC 27005:2022 Risk Manager, ki vključuje poglobljen pristop k informacijskim tveganjem ter uporabo mednarodno priznanih metodologij.

Na področju informacijske varnosti izvajajo ISO/IEC 27001 Lead Implementer in ISO/IEC 27001 Lead Auditor. Prvi je namenjen vzpostavitvi in upravljanju sistema varovanja informacij, drugi pa načrtovanju in izvajanju presoj skladnosti z ISO/IEC 27001.

Vse bolj aktualno je tudi področje umetne inteligence, zato izvajajo ISO/IEC 42001 Foundation, Lead Implementer in Lead Auditor. Programi so namenjeni razumevanju, vzpostavitvi in presoji sistema upravljanja umetne inteligence.

Za področje varstva osebnih podatkov je na voljo GDPR – Certified Data Protection Officer, namenjen vsem, ki opravljajo ali bodo opravljali naloge DPO oziroma sodelujejo pri zagotavljanju skladnosti z GDPR. Tečaj GDPR enkrat letno izvajajo tudi v živo kot 4-dnevni seminar.

Vlaganje v znanje je vlaganje v varnost

Certificirani PECB tečaji, ki jih pri DATAINFO.SI izvajajo na podlagi partnerskega sodelovanja že od leta 2019, so priložnost za pridobitev mednarodno priznanih znanj in kompetenc. Znanje s področja ISO standardov, GDPR, informacijske varnosti, neprekinjenega poslovanja, tveganj in umetne inteligence je pogoj za odgovorno, varno in zaupanja vredno poslovanje.

Več informacij o tečajih je na voljo na www.datainfo.si. (P.R.)

DATAINFO.SI, d.o.o.
02 620 43 00
info@datainfo.si
https://datainfo.si

REKONO

Vas varnost stane strank?

Digitalna identiteta, avtomatizirano preverjanje uporabnikov in storitve zaupanja najvišje pravne veljave postajajo temelj sodobnih digitalnih storitev. Z njihovo povezavo lahko podjetja varnost in preprosto uporabniško izkušnjo zagotovijo hkrati in brez kompromisov.

Podjetja danes veliko vlagajo v razvoj digitalnih storitev, nato pa uporabnike pogosto izgubijo tik pred sklenitvijo posla. Razlog praviloma ni produkt ali storitev, temveč postopek. Podatki[1] to potrjujejo: v spletni prodaji ostane nedokončanih skoraj 70 % nakupov, v financah pa kar 68 % uporabnikov opusti namero, povprečno že po slabih 20 minutah. Med najpogostejšimi razlogi sta predolg postopek in preveč zahtevanih podatkov.

Eden največjih izzivov sodobnega digitalnega poslovanja je, kako uporabnikom zagotoviti hitro in preprosto digitalno izkušnjo ter hkrati izpolnjevati varnostne in regulatorne zahteve. Pogosto velja prepričanje, da večja varnost pomeni tudi bolj zapleten uporabniški proces.

Vodilna slovenska podjetja s pomočjo storitev Rekono to navidezno dilemo že uspešno presegajo. Rezultat so krajši postopki, manj administracije in višje stopnje konverzije. Ključna prednost je povezan ekosistem, ki temelji na treh ključnih gradnikih: digitalni identiteti, avtomatiziranem preverjanju uporabnikov ter storitvah zaupanja najvišje pravne veljave.

Digitalna identiteta kot temelj digitalnih storitev

Vsak popolnoma digitalni proces se začne pri vprašanju, kako zanesljivo potrditi identiteto uporabnika brez obiska poslovalnice ali izvajanja dodatnih korakov.

Digitalna identiteta je eden ključnih gradnikov sodobnih digitalnih storitev. Če je uporabnik preverjen na ustrezni ravni zaupanja, lahko podjetje celoten proces izvede na daljavo – od registracije in oddaje vloge do sklenitve pogodbe ali podpisa dokumentov.

Tukaj nastopi račun Rekono, ki omogoča uporabo digitalne identitete ravni zanesljivosti visoko, kar zmanjšuje potrebo po dodatnih preverjanjih in poenostavlja uporabniško izkušnjo. Takšna identiteta je tudi osnova za uporabo kvalificiranega elektronskega podpisa, ki ima skladno z evropsko uredbo eIDAS enak pravni učinek kot lastnoročni podpis.

Avtomatizirano preverjanje uporabnikov

Drugi ključni steber predstavlja avtomatizirano preverjanje fizičnih oseb in podjetij. Postopki KYC (Know Your Customer) in KYB (Know Your Business) podjetjem omogočajo preverjanje identitete strank, zastopnikov, lastniške strukture podjetij in dejanskih lastnikov.

Rekono postopke KYC in KYB v veliki meri avtomatizira. S povezavami do registrov in uradnih evidenc, kot je AJPES, se podatki preverjajo neposredno iz zanesljivih virov. S tem se zmanjša možnost napak ročnega preverjanja ter omogoči hitrejše vključevanje strank, saj se skrajša čas obdelave, posledično pa tudi zmanjša administrativno breme. Avtomatizacija prav tako omogoča lažje izpolnjevanje regulatornih zahtev in večjo sledljivost procesov.

Rešitev je na voljo tudi kot storitev na ključ z lastno blagovno znamko ('white label'). Celoten postopek KYC in KYB gostuje na infrastrukturi Rekono, podjetje pa ga vključi pod svojo celostno grafično podobo brez lastnega razvoja in vzdrževanja sistema. Ker je rešitev že vzpostavljena in skladna z regulatornimi zahtevami, je uvedba hitra, podjetje pa se lahko osredotoči na svojo osnovno dejavnost.

Storitve zaupanja najvišje pravne veljave

Digitalna identiteta in preverjanje uporabnikov sama po sebi še ne zagotavljata zaupanja vrednega digitalnega poslovanja. Na koncu mora biti mogoče dokazati avtorstvo dokumenta, njegovo integriteto in čas nastanka.

Prav to zagotavljajo storitve zaupanja, kot so kvalificirani elektronski podpisi, elektronski žigi in kvalificirani časovni žigi, ki omogočajo izvajanje postopkov na daljavo brez izgube pravne veljavnosti ter zmanjšujejo stroške upravljanja dokumentacije.

Na področju kvalificiranega elektronskega podpisovanja je Rekono eden od le treh javnih ponudnikov storitev zaupanja v Sloveniji, uvrščenih na evropsko listo zaupanja vrednih ponudnikov, ki potrjuje skladnost z najstrožjimi zahtevami evropske uredbe eIDAS. Kvalificirana digitalna potrdila za elektronsko podpisovanje izdajata še država prek sistema SI-TRUST (SIGEN-CA) in Halcom.

Zakaj je pravi čas za ukrepanje prav zdaj?

Evropska uredba eIDAS 2.0 in evropska denarnica za digitalno identiteto (EUDI) bosta v prihodnjih letih pomembno vplivali na način identifikacije uporabnikov in izvajanje digitalnih storitev po vsej Evropski uniji. Države članice morajo do 24. decembra 2026 prebivalcem zagotoviti vsaj eno denarnico EUDI, do 22. novembra 2027 pa bodo morali vsi ponudniki storitev, ki od uporabnikov zahtevajo močno avtentikacijo, omogočati prijavo z njo.

Rekono je sistem za sprejemanje denarnic EUDI pripravil že pred izidom prve denarnice. Podjetja tako lahko sprejemanje denarnice uredijo centralno prek računa Rekono – brez lastnega razvoja in brez integracij z denarnicami posameznih držav. Obstoječa povezava z Rekono se ohrani, denarnica pa postane pomembna dodatna možnost prijave. Tako lahko podjetja zahteve izpolnijo že pred zakonskim rokom, prijava in vključevanje strank pa postaneta hitrejša in uporabna tudi čezmejno.

Več na https://www.rekono.si/. (P.R.)

[1]Baymard Institute (2026). Reasons for Cart Abandonment – Why 70% of Users Abandon Their Cart (2025 data). Dostopno na: https://baymard.com/blog/ecommerce-checkout-usability-report-and-benchmark

Signicat (2022). Record number of European consumers abandon financial applications during onboarding. Dostopno na: https://www.signicat.com/press-releases/the-battle-to-onboard-2022

Rekono d. o. o.
Ukmarjeva ulica 2, 1000 Ljubljana
www.rekono.si
info@rekono.si

MAVE D.O.O.

Nasveti za dobro izbiro pametne ključavnice za vhodna vrata

Nepogrešljivi partner za pametne ključavnice ter RFID sisteme.

Če ostanemo pred zaprtimi vrati brez ključa, imamo otroke, ki počasi začenjajo samostojno raziskovati okolico ali smo lastniki najemniškega stanovanja, se hitro pojavi potreba po sistemu za odpiranje vrat brez ključa. Kako izbrati ustrezno pametno ključavnico, smo povprašali Matjaža Križmančiča, direktorja podjetja Mave d.o.o., ki z več kot 17-letnimi izkušnjami na tem področju pomaga številnim mojstrom, podizvajalcem ter posameznikom.

Imamo protivlomna vhodna vrata z ročajem na zunanji strani in iščemo sistem za odpiranje vrat brez ključev. Kaj nam svetujete?

Za odpiranje protivlomnih vrat priporočam uporabo pametnih ključavnic Nuki v kombinaciji s tipkovnico na PIN kodo in prstnim odtisom. Pametno ključavnico se namesti na cilinder na notranji strani vrat, brezžično tipkovnico pa na zunanjo stran. Princip delovanja pametne ključavnice je tak, da dobesedno vrti ključ, kot če bi to naredili ročno. S tem zaklepa, odklepa in odpira vrata.

Je pametna ključavnica Nuki primerna za namestitev na vsako ključavnico? Kakšni so pogoji za uporabo obstoječega ključa oz. cilindričnega vložka?

Pametno ključavnico Nuki lahko namestimo na večino ključavnic z evropskim cilindričnim vložkom. Pogoj za uporabo obstoječega cilindričnega vložka je ta, da mora omogočati odklepanje s ključem iz notranje strani, tudi če je zunaj vstavljen ključ. Če je ta pogoj izpolnjen, bo vedno omogočen tudi zasilni vstop z navadnim ključem. Če ta pogoj ni izpolnjen ter če ima obstoječa ključavnica na notranji strani gumb, je potrebna menjava cilindričnega vložka.

Kakšne možnosti imamo, če je potrebna menjava cilindra? Poskrbite vi tudi za zamenjavo in montažo?

Če je potrebna zamenjava cilindričnega vložka, lahko izberete pametno ključavnico Nuki Ultra, ki ima priložen modularni cilindrični vložek, ki ga je možno prilagoditi za uporabo na večini vrat. Nuki cilinder je nastavljiv in primeren za ključavnice z dolžino od 30 do 55 mm na zunanji strani vrat (od vijaka) ter 30 do 67,5 mm na notranji strani. Zamenjava cilindra je v večini

primerov enostavna in mobilna aplikacija Nuki lepo vodi uporabnika skozi celotni proces. V nekaterih primerih je pri protivlomnih vratih cilinder skrit pod dodatnim zaščitnim okovjem – v tem primeru se morate obrniti izbranega serviserja protivlomnih vrat ali ključavničarja.

Ali lahko odprem vrata iz notranje strani tudi brez uporabe elektronike?

Ja, pametne ključavnice Nuki je iz notranje strani vedno možno zavrteti ročno in s tem lahko hitro odklenemo ali zaklenemo vrata brez uporabe elektronike. Ročno odklepanje ali zaklepanje je celo priporočljivo, saj podaljša avtonomijo in življenjsko dobo baterije.

Kakšna je avtonomija baterije in kako vemo, da se bo baterija kmalu izpraznila?

Stanje baterije je vidno v aplikaciji, in ko nivo napolnjenosti pade na 20 %, prejmete sporočilo na telefon in po elektronski pošti. Isto velja tudi za tipkovnico ter senzor za vrata.
Nuki ključavnici PRO in Ultra je možno povezati direktno na domači internet (WiFi), brez potrebe po nakupu dodatnih modulov, in s tem boste vedno pravočasno obveščeni – tudi v primeru, da aplikacije ne uporabljate redno.

Kako se namesti zunanjo tipkovnico in kaj lahko naredim, če mi prstni odtis ne prime?

Nuki tipkovnico se običajno pritrdi kar s priloženim lepilnim lističem, ki zagotavlja kvalitetno namestitev tudi v primeru vročine, mraza in drugih dejavnikov, k tipkovnici pa so priloženi tudi vijaki. Povezava med tipkovnico in ključavnico je brezžična in temelji na Bluetooth komunikacji. Nuki ponuja tri tipe tipkovnic: Keypad, ki vsebuje le številčnico, Keypad 2, ki vsebuje številčnico in senzor za prstne odtise ter Keypad 2 NFC, ki omogoča tudi odpiranje s prislanjanjem telefona. Za oddajanje stanovanj najpogosteje zadostuje tipkovnica brez skenerja prstnih odtisov, za domačo uporabo pa je vstop s prstnimi odtisi zelo priročen. Vsak uporabnik pa mora imeti poleg prstnega odtisa tudi svojo 6-mestno PIN kodo, ki jo lahko uporabi, če slučajno prstni odtis ne prime.

Po čem se razlikujete od drugih prodajalcev podobne opreme?

Pametne ključavnice Nuki uporabljamo tudi na svojih vratih in poznavanje tehnologije je naša največja prednost. Svojim strankam pomagamo v primeru potreb po določenih naprednejših nastavitvah ter v primeru morebitnih težav. Če želite preveriti, kateri sistem je najprimernejši za vaš vhod, nas lahko pokličete ali pošljete povpraševanje in z veseljem vam bomo pomagali. (P.R.)

mave
Kartice in RFID sistemi

MAVE, Kartice in RFID sistemi, d.o.o .
Pod jezom 40,
1000 Ljubljana
Tel.: +386 41 884 124
e-pošta: info@mave.si
www.mave.si

Plačujte, varčujte in trgujte v NLB Kliku.

Že več kot 500.000 ljudi svoje bančne storitve opravlja **v najboljši digitalni banki* NLB Klik**, ki zagotavlja zanesljivo izkušnjo, s sodobnimi varnostnimi rešitvami, identifikacijo z video klicem in podporo NLB Kontaktnega centra pa vam je na voljo 24/7.
Tudi če ste na plaži.

Digitalna banka št. 1*

*Raziskava E-laborat, 2025

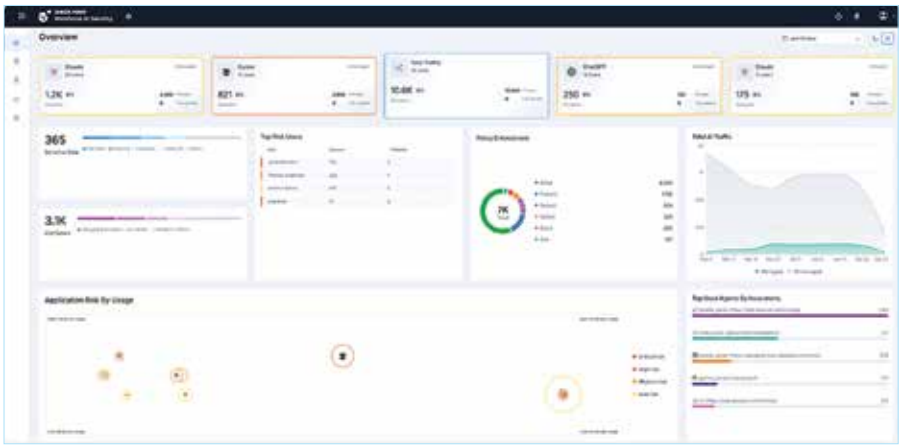
NLB

CHECK POINT WORKFORCE AI SECURITY

Zaposleni uporabljajo UI orodja. Ali podjetja vedo, kaj se dogaja v ozadju?

Generativna umetna inteligenca je postala nepogrešljiva v marsikaterem delovnem okolju.

Orodja, kot so ChatGPT, Copilot, Gemini in Claude, zaposlenim pomagajo pri pripravi besedil, analizi podatkov, programiranju, raziskovanju in avtomatizaciji vsakodnevnih nalog. Podjetja zato v svoje procese pospešeno uvajajo umetno inteligenco, saj želijo povečati produktivnost in konkurenčnost.



Ali imajo organizacije pregled nad uporabo umetne inteligence?

Ali imajo organizacije sploh pregled nad tem, kako zaposleni uporabljajo umetno inteligenco in katere podatke pri tem delijo z različnimi UI-sistemi? Podobno kot se je pred leti pojavil pojav »Shadow IT«, ko so zaposleni brez vednosti IT oddelka uporabljali različne spletne storitve in aplikacije, danes govorimo o »Shadow AI«. Zaposleni pogosto uporabljajo javno dostopna orodja umetne inteligence, ne da bi organizacija za to vedela.

Nepremišljena uporaba vodi v tveganje

In prav tu se začnejo največja tveganja. Umetna inteligenca je izjemno uporabna, vendar lahko nepremišljena uporaba povzroči razkritje občutljivih poslovnih informacij, osebnih podatkov strank, finančnih podatkov ali izvorne kode programskih rešitev. Dovolj je, da zaposleni v pogovorno okno vnese pogodbo, interni dokument ali del programske kode in podjetje lahko v hipu izgubi nadzor nad pomembnimi informacijami. Posebej občutljivo področje predstavljajo razvojni oddelki. Programerji vse pogosteje uporabljajo pomočnike za pisanje kode, kot so GitHub Copilot, Cursor in podobna orodja. Čeprav ta pomembno pospešijo razvoj programske opreme, se hkrati pojavljajo vprašanja o zaščiti intelektualne lastnine, zaupnih podatkov in skladnosti z internimi varnostnimi politikami.

Poleg tega umetna inteligenca ni več omejena zgolj na odgovarjanje na vprašanja uporabnikov. V ospredje prihajajo tako imenovani AI-agenti, ki lahko izvajajo konkretna dejanja, dostopajo do poslovnih sistemov, uporabljajo podatke iz različnih virov in samostojno opravljajo naloge. Takšen razvoj prinaša nove priložnosti, hkrati pa tudi nova varnostna tveganja.

Kako umetno inteligenco uporabljati varno?

Če je bilo še pred kratkim glavno vprašanje, ali bodo podjetja uporabljala umetno inteligenco, je danes pomembnejše, kako jo uporabljati varno. Klasične varnostne rešitve pogosto ne zagotavljajo zadostnega vpogleda v UI-interakcije, saj niso bile zasnovane za okolje, v katerem zaposleni komunicirajo z desetinami različnih modelov in storitev umetne inteligence.

Zato se na trgu pojavljajo specializirane platforme za upravljanje in zaščito uporabe umetne inteligence. Workforce AI Security podjetja Check Point na primer organizacijam omogoča pregled, upravljanje in zaščito uporabe umetne inteligence v delovnem okolju.

Kako deluje Workforce AI Security?

Rešitev je mogoče aktivirati prek lahke razširitve za spletni brskalnik, zato podjetjem ni treba izvajati zapletenih sprememb omrežne infrastrukture ali preoblikovati obstoječega IT-okolja. Poleg spletnih storitev rešitev podpira tudi nadzor uporabe umetne inteligence v namiznih aplikacijah, razvojnih okoljih in programerskih pomočnikih za pisanje kode.

Sicer pa Workforce AI Security temelji na treh ključnih področjih. Prvo je odkrivanje uporabe umetne inteligence. Organizacija oziroma administrator v konzoli vidi, katera UI-orodja zaposleni uporabljajo, kako pogosto jih uporabljajo in katere vrste podatkov se pri tem obdelujejo. Sistem zazna tako odobrena kot tudi neodobrena orodja in pomaga odkriti morebitne slepe pege v organizaciji.

Drugo področje predstavlja upravljanje. Skrbniki lahko določijo podrobna pravila glede uporabe posameznih UI-storitev, tipov podatkov in uporabniških skupin. Tako je mogoče zagotoviti, da uporaba umetne inteligence ostane skladna z internimi politikami podjetja ter regulatornimi zahtevami.

Tretji steber je zaščita podatkov. Sodobne rešitve za varovanje uporabe UI imajo napredne mehanizme za preprečevanje uhajanja podatkov, prepoznavanje občutljivih vsebin in nadzor nad informacijami, ki jih uporabniki pošiljajo v sisteme. Med drugim lahko zaznajo osebne podatke, poslovne skrivnosti, finančne informacije ali programsko kodo ter preprečijo njihovo nepooblaščeno deljenje.

Umetna inteligenca bo v prihodnjih letih postala sestavni del skoraj vsakega poslovnega procesa. Organizacije zato ne smejo razmišljati zgolj o tem, kako zaposlenim omogočiti uporabo novih tehnologij, temveč tudi o tem, kako zagotoviti ustrezno raven varnosti, nadzora in skladnosti. (P.R.)

TERATEC

Med vašim dopustom tatovi »delajo«, bodite pripravljeni

Predstavljajte si, da se pozno zvečer vrnete domov. Vse je na videz v redu, a občutek nelagodja ne izgine. Ste res lahko povsem mirni?

Vlomi so vse pogostejši, tatovi pa vse drznejši, zato dom ni več samoumevno varen prostor. Vlom ali zgolj zavedanje, da je nekdo brskal po vaših stvareh, občutek varnosti v hipu poruši. In prav zato se vse več ljudi odloča, da ne bo več zgolj upalo na srečo, temveč bo varnost svojega doma vzelo v svoje roke. Tehnično varovanje ni znak strahu, temveč premišljena odločitev za mirnejše življenje.

Tatove zanimajo prav vsi domovi

Vlomilci ne izbirajo več le zapuščenih hiš ali očitno premožnih tarč. Pogosto jih zanimajo prav običajni domovi, kjer računajo na presenečenje in hiter umik. Ključavnica in zaklenjena vrata jih ne ustavijo za dolgo.

Protivlomni sistemi Teratec so zasnovani tako, da nepridiprave odkrijejo takoj. Glasen alarm, takojšnje obvestilo na vaš pametni telefon in zavedanje, da je nekdo zaznal njihovo prisotnost, večino vlomilcev odvrne, še preden pride do resne škode. Občutek nadzora dodatno okrepi videonadzor. Kamere visoke ločljivosti omogočajo spremljanje dogajanja okoli hiše in v njej, podnevi in ponoči, v vseh vremenskih razmerah. Ne gre zgolj za posnetke, temveč za možnost, da v vsakem trenutku preverite, kaj se dogaja doma. Ste na dopustu? V službi? Na izletu? Pogled v aplikacijo vam v nekaj sekundah pove, ali je vse tako, kot mora biti. In ta občutek je neprecenljiv.

Varnost lahko ogrozi tudi požar, poplava …

Varnost doma pa ne ogrožajo samo vlomi. Požar, ki se lahko razvije neopazno in izjemno hitro, predstavlja eno največjih groženj za dom in družino. Sistemi za zgodnje zaznavanje požara omogočajo, da ste o nevarnosti obveščeni pravočasno, ko je še mogoče ukrepati. Ko so protivlomni alarmi, videonadzor, požarni senzorji in senzorji za zaznavanje vode povezani v enoten sistem, dobimo pametno rešitev, ki deluje samodejno in zanesljivo tudi takrat, ko vas ni doma.

Teratec poskrbi za vse

Sistemi so prilagodljivi, primerni tako za stanovanja kot za hiše. Upravljanje je preprosto in brez zapletenih nastavitev, pomoč strokovnjakov pa je vedno na voljo. Teratec poskrbi za vse – od prvega nasveta in načrtovanja do vgradnje, zagona sistema in dolgoročne podpore. Brez skritih stroškov in brez neprijetnih presenečenj.

> Tehnično varovanje doma je naložba v miren spanec, brezskrbne počitnice in občutek, da vaš dom ni lahka tarča. Tatovi namreč vedno iščejo najlažjo pot – in dobro zaščiten dom to zagotovo ni.

Zaščitite tudi poslovni prostor ali objekt

Teratecove rešitve pa niso namenjene zgolj domovom. Lastniki in upravitelji poslovnih prostorov, pisarn ali manjših objektov lahko izkoristijo iste napredne tehnologije, prilagojene specifičnim poslovnim potrebam. Poleg tega so v poslovnem okolju pogosto v ospredju kontrola pristopa, ki omogoča natančno upravljanje pravic zaposlenih in obiskovalcev, ter biometrične rešitve, ki zagotavljajo dodatno raven varnosti. Video nadzor se v poslovnih prostorih uporablja tako za zunanji nadzor površin kot za spremljanje notranjih prostorov. Poleg tega Teratec ponuja tudi integracijo požarnih sistemov in sistemov javljanja nevarnosti, s čimer poslovnim objektom zagotavlja neprekinjeno delovanje in pravočasno reakcijo v primeru izrednih razmer.

Opremite svoj dom s sistemom tehničnega varovanja. Družina vam bo hvaležna. In pes tudi.

Če razmišljate, kako bolje zaščititi svoj dom ali poslovni prostor, je zdaj pravi trenutek za odločitev. Ne čakajte, da vas k temu prisili neprijeten dogodek. Oglejte si rešitve podjetja Teratec na spletni strani www.teratec.si in naredite prvi korak k varnosti še danes. (P.R.)

TECH TRADE TRZIN

Ko nevidno postane vidno z optično tehnologijo

Tam, kjer se človeško oko sooči z naravnimi fizikalnimi omejitvami, najsi bo to zaradi trdnih ovir, popolne teme ali nevidnega infrardečega sevanja, na prizorišče stopijo napredne slikovne naprave.

Pregreta električna povezava, vlažen del stene, zamašena cev, poškodovan prezračevalni kanal ali težko dostopen motorni sklop pogosto nase ne opozorijo takrat, ko je popravilo še enostavno. Vidni znaki se pojavijo pozneje, ko je strošek večji, poseg zahtevnejši in izpad delovanja daljši. Zato imajo mojstri v svojem repertoarju termovizijske, endoskopske in nočne kamere, s katerim nevidno postane vidno.

Tech Trade Trzin v svoji ponudbi združuje več takšnih rešitev, ki uporabniku omogočijo vpogled tja, kamor običajen pogled ne seže. Termovizijska kamera pokaže temperaturne razlike, endoskopska kamera omogoči pregled ozkih in skritih prostorov, nočni daljnogled pa razširi uporabnost opazovanja tudi v slabih svetlobnih pogojih.

Temperatura kot diagnostični podatek

Termovizijska kamera ne prikazuje klasične slike prostora, temveč zaznava infrardeče sevanje, ki ga oddajajo površine. Ker se količina tega sevanja spreminja s temperaturo, lahko kamera temperaturne razlike pretvori v barvno sliko. Na ta način uporabnik hitro opazi vroče točke, hladne mostove, slabo izolirane dele, pregrete kontakte ali neenakomerno delovanje ogrevalnih in hladilnih sistemov.

FNIRSI TDM-120 je primer samostojne termovizijske kamere, ki je zasnovana za servisne, industrijske, gradbene in vzdrževalne preglede. Uporablja IR ločljivost 120×90, vanadijev oksidni detektor, 2,8-palčni LCD zaslon na dotik in temperaturno območje od –20 do 400 °C. Pomembna prednost je tudi samodejno sledenje najvišji in najnižji temperaturi, saj uporabniku ni treba ročno iskati najbolj kritičnega dela prizora.

Za uporabnike, ki želijo bolj kompaktno rešitev, je zanimiva termovizijska kamera Habotest HT820. Ta se prek priključka USB-C poveže na Android telefon in ga spremeni v prenosno termovizijsko orodje.

Endoskopska kamera za prostore, kamor roka ne seže

Druga vrsta uporabnega pregleda je vizualni dostop do skritih mest. Pri ceveh, motornih sklopih, prezračevanju, odtokih, stenah, gospodinjskih napravah ali strojnem vzdrževanju se pogosto zgodi, da napake ni mogoče preveriti brez razstavljanja. Endoskopska kamera je pri tem praktičen vmesni korak, saj omogoča pregled notranjosti brez večjega posega.

Ancel W655 uporablja 5,5-milimetrsko sondo in 5-metrski poltrdi kabel, kar omogoča dostop do ozkih in oddaljenih mest. Slika se prek Wi-Fi povezave prenaša na mobilno napravo (Android ali iOS), kamera pa omogoča zajem slike in videa do ločljivosti 1920×1080. Zaradi zaščite IP67 je primerna tudi za uporabo v vlažnih okoljih, priloženi nastavki, kot so ogledalo, kljuka in magnet, pa povečajo uporabnost pri iskanju, pobiranju ali pregledu predmetov na nedostopnih delih.

Takšna kamera ni namenjena samo profesionalnim serviserjem. Uporabna je tudi pri domačih popravilih, preverjanju odtokov, pregledu za pohištvom, v avtomobilu ali pri manjših inštalacijskih posegih.

Popolna jasnost v temi s pomočjo infrardečega spektra

Tretji steber napredne optike predstavlja digitalni nočni vid. FNIRSI NVS-20 je digitalni nočni daljnogled, ki omogoča snemanje v ločljivosti 4K in zajem fotografij do ločljivosti 36 MP.

Za razliko od klasičnih analognih naprav za nočni vid, ki delujejo na principu ojačevanja preostale svetlobe, digitalni sistemi uporabljajo visoko občutljive senzorje v kombinaciji z vgrajenim infrardečim osvetljevalcem valovne dolžine 850 nanometrov. Ta svetloba je človeškemu očesu povsem nevidna, omogoča pa opazovanje v popolni temi na razdalji do 300 metrov. Naprava ponuja 6-kratno digitalno povečavo in sedem stopenj nastavljive infrardeče osvetlitve, kar omogoča prilagoditev vsem svetlobnim pogojem.

Kampiranje, lovstvo, opazovanje divjih živali v naravnem okolju, reševalne misije … To je le nekaj scenarijev, v katerih boste raje kot po klasični svetilki posegli po nočnem daljnogledu.

Zakaj bi ugibali, kaj je pred vami

Ko je mogoče temperaturno odstopanje prepoznati še pred okvaro, notranjost cevi ali naprave pregledati brez nepotrebnega razstavljanja, dogajanje v temi pa zabeležiti brez ugibanja, se ugibanje spremeni v razumevanje in hitrejše ukrepanje. Več lahko najdete na spletni strani www.techtrade.si. (P.R.)

TECHTRADE
www.techtrade.si

TECH TRADE d.o.o. Trzin
Blatnica 8, 1236 Trzin
+386 1 562 21 11

KIBERNETSKA VARNOST NI VEČ VPRAŠANJE, ALI – TEMVEČ KDAJ.

Ko napadalci delujejo 24 ur na dan, mora enako delovati tudi vaša zaščita.

V T-2 za varnost poslovnih okolij skrbi ekipa vrhunskih strokovnjakov iz lastnega **Security Operations Centra (SOC)** in **Nadzorno operativnega centra (NOC)**, ki neprekinjeno, **24 ur na dan, 7 dni v tednu,** spremlja delovanje informacijskih sistemov, zaznava varnostne incidente ter zagotavlja hiter odziv.

- 24/7 spremljanje varnostnih dogodkov
- celovita zaščita omrežij, naprav, uporabnikov in podatkov
- hitra analiza in odzivanje na incidente
- podpora pri zahtevah NIS2, DORA in drugih regulativah

»Največja prednost ni tehnologija. Največja prednost so ljudje.«

"Kibernetske grožnje se razvijajo vsak dan, zato jih lahko učinkovito obvladuje le izkušena ekipa strokovnjakov, ki sisteme spremlja neprekinjeno. V T-2 združujemo napredne tehnologije in znanje naših analitikov, kar našim naročnikom omogoča hitro zaznavo ter odziv na varnostne incidente."

Marko Doltar
vodja NOC in SOC, T-2

»Za vsakim opozorilom stoji strokovnjak.«

"SOC ni zgolj sistem za spremljanje dogodkov. Je ekipa ljudi, ki razume delovanje informacijskih okolij, prepoznava kompleksne napade in pomaga podjetjem sprejemati prave odločitve ob pravem času. Naš cilj je, da se uporabniki lahko posvetijo svojemu poslu, za varnost pa poskrbimo mi."

Lucija Starc
prodajna inženirka za kibernetsko varnost in SOC analitičarka, T-2

Kibernetska varnost je proces. Ne enkratna odločitev.

V T-2 vam razvijemo kibernetsko rešitev po meri, prilagojeno vašemu podjetju – ne glede na njegovo velikost. Z vrhunskim strokovnim znanjem, lastnim SOC centrom in naprednimi tehnologijami poskrbimo za proaktivno zaščito, hiter odziv in varno poslovanje.

Želim posvet

INFO-KOD D.O.O.

Kdaj je čas za prehod na industrijski tiskalnik nalepk?

V številnih podjetjih je bilo tiskanje nalepk dolgo časa obravnavano kot podporni proces – nekaj, kar "mora delovati".

Z rastjo poslovanja, večanjem obsega logistike in zahtevami po sledljivosti izdelkov postaja jasno, da ima izbira prave tiskalne infrastrukture pomemben vpliv na učinkovitost poslovanja.
Ko podjetje preide iz nekaj deset na več sto ali celo tisoče natisnjenih nalepk dnevno, se dinamika dela spremeni. Večja frekvenca tiskanja pomeni večjo obrabo komponent, pogostejše menjave potrošnega materiala in večjo verjetnost zastojev.
V logistiki, proizvodnji ali distribuciji lahko že kratka prekinitev zaradi menjave role ali okvare vpliva na celoten delovni tok. Industrijski tiskalniki so bili razviti prav za takšne scenarije.

Razlika med industrijskim in namiznim tiskalnikom

Glavna razlika ni zgolj v hitrosti tiskanja. Industrijski modeli so zasnovani za bistveno višje delovne obremenitve, daljše neprekinjeno delovanje in večjo mehansko vzdržljivost.
Večja kapaciteta rol nalepk in termo trakov pomeni manj menjav in manj prekinitev dela. Robustna konstrukcija, pogosto kovinska, omogoča uporabo v zahtevnejših okoljih, kot so proizvodne hale, skladišča ali distribucijski centri.
Pomembna prednost je tudi natančnost. Pri tisku črtnih kod, serijskih številk, QR kod ali GS1 2D kod je kakovost izpisa ključna za nemoteno delovanje skenerjev in sledilnih sistemov.
Industrijski tiskalniki omogočajo širšo integracijo v poslovne sisteme, kot so ERP, WMS in MES, ter podporo naprednim funkcionalnostim, kot sta RFID označevanje in avtomatsko apliciranje nalepk.
Kdaj pa je smiseln prehod na industrijski tiskalnik? Predvsem takrat, ko dnevni obseg tiskanja presega nekaj sto etiket in tiskalnik deluje več ur neprekinjeno. Na potrebo po nadgradnji opozarjajo tudi prepogoste menjave materiala, zahteve po boljši sledljivosti, zahtevni delovni pogoji (prah, toplota ali vlaga) ter vse višji stroški zaradi zastojev v proizvodnji.

Zebra kot industrijski standard

Med najbolj prepoznavnimi proizvajalci na področju industrijskega označevanja ostaja Zebra Technologies, katere rešitve so prisotne v logistiki, zdravstvu, proizvodnji in maloprodaji po vsem svetu. Posebnost Zebra industrijskih tiskalnikov je modularna zasnova. Podjetje ne izbira zgolj osnovnega modela, temveč celotno konfiguracijo glede na specifične potrebe.
Na voljo sta dve različni tehnologiji tiska: **direktni termalni (DT)** za kratkotrajne logistične etikete brez uporabe traku; **termo transferni (TT)** za trajnejše oznake, odporne na toploto, vlago in mehanske vplive.

ZEBRA ZT231 ZEBRA ZT411 ZEBRA ZT620

Prav tako so na voljo različne ločljivosti – od standardnih 203 dpi do 300 dpi, pri določenih modelih pa tudi 600 dpi za mikro etikete, drobne črtne kode ali farmacevtske aplikacije.
Pomemben del konfiguracije predstavljajo dodatni moduli:

- **Odlepljevalec** za avtomatsko ločevanje nalepk,
- **Rezalnik** za samodejno rezanje etiket,
- **Navijalnik** za avtomatsko navijanje nosilnega materiala,
- **Wi-Fi** in dodatni mrežni moduli za lažjo integracijo v omrežje.

Zebra ZT231: prvi korak v industrijsko okolje

Zebra ZT231 predstavlja vstopni industrijski razred. Ponuja hitrost do 305 mm/s, podporo za širino tiska do 104 mm ter možnost izbire med 203 in 300 dpi. Standardno vključuje USB, serijski in Ethernet priklop, z možnostjo kasnejših nadgradenj, kot so peeler, cutter, Wi-Fi ali RFID. Njegova velika prednost je prav možnost postopne nadgradnje brez menjave celotnega sistema. Primeren je predvsem za skladišča, logistiko, osnovno proizvodnjo, interno označevanje.

Zebra ZT411: ko proces zahteva več

Zebra ZT411 je naslednji korak za podjetja, kjer je tiskanje že kritični del operacije. Poleg večjih hitrosti (do 356 mm/s) omogoča širši nabor resolucij, vključno s 600 dpi. Na voljo so tudi naprednejše konfiguracije, kot so full-roll rewinder, RFID za kovinske oznake ter bolj kompleksne integracije v avtomatizirane linije.
ZT411 pogosto najdemo v farmaciji, avtomobilski industriji, zahtevnejši proizvodnji, velikih distribucijskih sistemih.

Zebra ZT600 serija: za kritične procese

Zebra ZT600 Series predstavlja najvišji industrijski razred. Modeli v tej seriji so namenjeni 24/7 delovanju v okoljih, kjer izpad pomeni neposredno poslovno izgubo.
ZT610 in ZT620 omogočata izredno visoko natančnost, robustno kovinsko konstrukcijo, večjo notranjo zmogljivost pomnilnika, višje hitrosti ter napredno upravljanje. Posebej izstopa možnost 600 dpi pri modelu ZT610 za mikro označevanje v elektroniki ali farmaciji.

Tiskanje kot strateški del procesov

Pravilna izbira tiskalne opreme vpliva na produktivnost, zmanjšanje napak, sledljivost in dolgoročne stroške.
Zato se ne sprašujte, ali boste morali za industrijski tiskalnik odšteti več. Vprašajte se, koliko boste izgubili, če ga potrebujete, pa ga še nimate. (P.R.)

ANNI D.O.O.

En klik. Ena napaka. Velike posledice.

Direktor je na službeni poti. Računovodkinja prejme elektronsko sporočilo z njegovo fotografijo in podpisom. Sporočilo je kratko: "Prosim, nujno preverite dokument in potrdite plačilo."

Pošiljatelj je videti pravi. Besedilo nima slovničnih napak. Vse deluje povsem običajno.
Klik.
V nekaj trenutkih napadalci pridobijo dostop do uporabniškega računa in začne se ena najpogostejših zgodb sodobnih kibernetskih incidentov. Takšni primeri danes niso več izjema. So vsakodnevna realnost podjetij vseh velikosti. Kibernetski kriminalci so ugotovili, da je pogosto precej lažje pretentati človeka kot zaobiti napredno varnostno infrastrukturo.
Zato danes največja ranljivost podjetja ni več strežnik ali aplikacija – temveč uporabnik.

Varnost lahko tudi izmerimo

Hornetsecurity Security Awareness Service ni le platforma za izvajanje e-izobraževanj. Gre za rešitev, ki podjetjem omogoča merjenje dejanskega varnostnega vedenja zaposlenih.
S pomočjo simulacij phishing napadov, interaktivnih izobraževanj in napredne analitike organizacije dobijo realno sliko o tem, kako se njihovi zaposleni odzivajo na sodobne kibernetske grožnje.
Osrednji kazalnik je **Employee Security Index (ESI)** – varnostni indeks zaposlenih, ki z oceno od 0 do 100 prikazuje stopnjo njihove varnostne ozaveščenosti. Višja kot je vrednost, bolje zaposleni prepoznavajo nevarnosti in sprejemajo varne odločitve.
Podjetje tako prvič dobi odgovor na vprašanje: Kje smo danes in kako uspešni smo pri izboljševanju varnostne kulture?

Podatki, ki povedo več kot občutek

Platforma omogoča spremljanje številnih kazalnikov, med drugim:

- **Employee Security Index (ESI)** za posameznike, skupine in celotno organizacijo,
- uspešnost simuliranih phishing kampanj,
- koliko uporabnikov je kliknilo na povezavo, odprlo priponko ali vneslo poverilnice,
- koliko zaposlenih je sumljivo sporočilo pravilno prijavilo,
- katere psihološke prijeme (nujnost, avtoriteta, radovednost …) napadalci najlažje izkoristijo,
- primerjavo med oddelki in ekipami,
- napredek posameznikov skozi čas.

Takšen vpogled omogoča, da podjetja usposabljanja usmerijo tja, kjer jih najbolj potrebujejo.

Napaka ni neuspeh – je priložnost za učenje

Ena največjih prednosti rešitve je pristop *Teachable Moments*.
Če uporabnik med simulacijo nasede phishing sporočilu, ga sistem ne kaznuje. Takoj se odpre kratka izobraževalna stran, ki pojasni, kateri znaki so nakazovali prevaro in kako bi jo lahko naslednjič prepoznal.
Prav takšno učenje v trenutku, ko se napaka zgodi, dokazano najbolj učinkovito spreminja vedenje zaposlenih.

Izobraževanje, prilagojeno uporabnikom

Security Awareness Service vključuje obsežno knjižnico interaktivnih e-treningov, ki so na voljo tudi v slovenskem jeziku.
Uporabniki napredujejo po petih stopnjah znanja, sistem pa glede na njihove rezultate sam prilagaja zahtevnost vsebin. Vodstvo lahko spremlja napredek posameznikov in skupin, primerja oddelke ter dodeljuje ciljno usmerjena izobraževanja tam, kjer je tveganje največje.
Namesto enkratnega letnega predavanja tako podjetje vzpostavi neprekinjen proces razvoja varnostne kulture.

Od tehnologije do ljudi

V podjetju Anni organizacijam pomagajo pri uvajanju rešitve Hornetsecurity **Security Awareness Service** ter pri oblikovanju programov ozaveščanja, ki temeljijo na dejanskih podatkih, ne ugibanjih. Ker je danes človek najpogostejša tarča kibernetskih napadov, postaja merjenje in izboljševanje njegove pripravljenosti ena najpomembnejših naložb v informacijsko varnost. Prava vrednost rešitve ni le v tem, da zaposlene izobražuje, temveč da podjetju pokaže, kako se njihova varnostna kultura razvija – in kje so še priložnosti za izboljšave.

Ste pripravljeni preveriti, kako varni so vaši zaposleni?

V podjetju Anni vam pomagajo vzpostaviti program ozaveščanja zaposlenih s pomočjo rešitve Hornetsecurity Security Awareness Service. Skupaj z njimi lahko izmerite trenutno raven varnostne kulture, pripravite ciljno usmerjena usposabljanja in zmanjšate tveganje za uspešne phishing napade. (P.R.)

HORNETSECURITY
BY proofpoint.

anni
www.anni.si

Anni d.o.o.
Motnica 7a, Trzin,
T: 01/ 5800 800 • info@varen.it

JUNIPER EXPERIENCE

Vse več podjetij pri upravljanju omrežij stavi na AI

Podjetja potrebujejo hitra, varna in zanesljiva omrežja, ki se znajo prilagajati vedno večjim zahtevam uporabnikov, hibridnemu načinu dela ter vse večji uporabi storitev v oblaku.

Pri tem postajata pomembni tudi avtomatizacija upravljanja ter uporaba umetne inteligence za hitrejše odkrivanje in odpravljanje težav.
Podjetje Infinigate kot uradni zastopnik rešitev Juniper Networks zato predstavlja svoje strokovno in demonstracijsko okolje, kjer lahko slovenska podjetja in IT strokovnjaki iz prve roke spoznajo najsodobnejše omrežne tehnologije tega globalnega ponudnika in inovatorja. Juniper Networks, ki je danes del skupine HPE, že desetletja postavlja standarde na področju naprednih omrežij, varnosti in umetne inteligence v omrežni infrastrukturi.

Zakaj Juniper Networks? Inteligentna omrežja naslednje generacije

Juniper Networks je prepoznaven po svojem inovativnem pristopu, ki združuje visoko zmogljivost, avtomatizacijo in umetno inteligenco. Njihove rešitve so namenjene podjetjem vseh velikosti, podatkovnim centrom, javnim ustanovam in organizacijam, ki želijo zgraditi sodobno, varno in učinkovito omrežno infrastrukturo.
Portfelj rešitev vključuje:

- AI-Native Networking (Mist AI) – napredno upravljanje omrežij z umetno inteligenco, ki omogoča proaktivno odkrivanje težav, samodejno optimizacijo delovanja ter vrhunsko uporabniško izkušnjo.
- Napredne Wi-Fi rešitve (Wi-Fi 6E in Wi-Fi 7) – visoko zmogljiva brezžična omrežja z nizko latenco in zanesljivo povezljivostjo za sodobna digitalna okolja.
- Visoko zmogljiva stikala (seriji EX in QFX) – zasnovana za podatkovne centre, kampus omrežja in enterprise okolja.
- SD-WAN in varnostne rešitve (serija SRX) – celovita zaščita omrežja z integrirano inteligenco in avtomatizacijo.
- Cloud-native upravljanje (Juniper Mist Cloud) – enotna platforma za upravljanje celotnega omrežja iz oblaka, ki omogoča popoln pregled nad delovanjem infrastrukture in nadzor ne glede na lokacijo.

> Juniper Networks je prepoznaven po svojem inovativnem pristopu, ki združuje visoko zmogljivost, avtomatizacijo in umetno inteligenco.

Pomemben mejnik predstavlja tudi združitev podjetij HPE in Juniper Networks, s katero se odpira nova era integriranih IT rešitev, ki uporabnikom prinaša še tesneje povezane rešitve za podatkovne centre, omrežja, oblak in varnost. Integriran ekosistem podjetjem omogoča hitrejšo digitalno preobrazbo, učinkovitejše upravljanje IT okolja ter izboljšano uporabniško izkušnjo.

Juniper Experience okolje – prostor inovacij, testiranja in znanja

Izbira omrežne infrastrukture je dolgoročna odločitev, zato je pomembno, da lahko podjetja tehnologijo preizkusijo še pred uvedbo v produkcijsko okolje. Prav temu je namenjeno demonstracijsko okolje Juniper Experience.
Obiskovalci lahko v realnih scenarijih spoznajo delovanje najnovejših rešitev Juniper Networks ter se prepričajo o njihovih zmogljivostih in prednostih. Demonstracijsko okolje omogoča praktičen vpogled v sodobne pristope k upravljanju omrežij.
Na voljo so:

- praktično testno okolje z dostopom do najnovejših rešitev Juniper Mist AI, naprednih dostopnih točk, stikal in varnostnih platform;
- prikaz konkretnih primerov uporabe v kampus omrežjih, podatkovnih centrih ter hibridnih in cloud okoljih;
- možnost izvedbe pilotnih projektov in testnih implementacij, s katerimi lahko podjetja preverijo delovanje rešitev v svojem dejanskem IT okolju še pred končno investicijsko odločitvijo.

Demonstracijsko okolje je namenjeno tako poslovnim partnerjem kot podjetjem, ki želijo posodobiti svojo omrežno infrastrukturo, izboljšati uporabniško izkušnjo in izkoristiti prednosti upravljanja omrežij s pomočjo umetne inteligence. Juniper Experience tako predstavlja prostor, kjer se teorija sreča s prakso. (P.R.)

Infinigate d.o.o.
Ukmarjeva 4
1000 Ljubljana

0590 14914
info.si@infinigate.com

www.infinigate.com/si

SUBRÍNA RECEPT

KATERI PROBLEM LASIŠČA IMAŠ TI?

MASTNI LASJE

SRBEČE LASIŠČE

IZPADANJE LAS

PRHLJAJ

UČINKOVITE FORMULE V SODELOVANJU ZNANJA IN NARAVE

ACORD-92

Tehnologija je popolnoma spremenila poslovne prostore in učilnice

Predavalnice, učilnice in konferenčne sobe so v zadnjih nekaj letih dobile povsem drugačno podobo, kot so jo imele še pred desetletjem. Skupni imenovalec teh sprememb je tehnologija.

Tehnološke rešitve zaradi vseh prednosti, ki jih nudijo pri izobraževanju in v poslu, počasi osvajajo tudi tiste najbolj skeptične uporabnike. Ko enkrat preizkusimo velike zaslone, občutljive na dotik in odkrijemo možnosti modernih projektorjev ter videokonferenčnih sistemov, si preprosto ne moremo več predstavljati, kako smo živeli brez njih.

Kar je pri sodobni učilnici najpomembneje izpostaviti, so prav olajšana komunikacija, sodobni interaktivni monitorji, ki jo dopolnjujejo in podobne rešitve.

Če omenimo nekaj imen, ki briljirajo na tem področju, zagotovo ne moremo mimo velikih igralcev, kot so **Viewsonic**, **Iiyama**, **Hikvision**, **BenQ** in **Sharp**. Podjetje Acord-92 je dobavitelj vseh omenjenih znamk in nudi celovito ponudbo in storitev z možnostjo montaže in servisa izdelkov ter celo izobraževanja zanje.

Snovalci modernih tehnoloških rešitev se sicer trudijo, da poskrbijo za enostavno namestitev ter uporabniško dovršene in prijazne uporabniške vmesnike, a tudi ti se med seboj razlikujejo. Prav tako so nekateri ljudje za novosti bolj dovzetni, drugi manj. Zato pri Acord-92 poskrbijo, da pred rešitvami, ki vam bodo olajšale delo, ne bežite, temveč vas izobrazijo, da vam bodo v veselje.

Interaktivni zasloni na dotik in projektorji

Interaktivni zasloni podjetja **Viewsonic** ločljivosti 4K in občutljivi na dotik ponujajo neverjetno digitalno izkušnjo. So kot nalašč za moderne poslovne prostore in učilnice. Kakovostni zasloni s sliko, ostro kakor britev, ki so občutljivi na dotik, nudijo podporo za dve pisali hkrati, imajo možnost deljenja zaslona na več delov, vgrajene kakovostne zvočnike, možnost deljenja vsebine in imajo intuitivni uporabniški vmesnik, so kombinacija, ki vas bo navduševala še dolgo po nakupu. Podjetje **Viewsonic** se lahko pohvali tudi s kakovostnimi projektorji in monitorji.

Potem je tu podjetje **Iiyama**, ki je danes eden večjih proizvajalcev računalniških monitorjev, prav tako pa je znano kot odličen proizvajalec zaslonov na dotik, ki je uspešen prav zaradi dolgoletnega razvoja visoko kakovostnih izdelkov, ki jih ponuja po dostopni ceni. Ko beseda nanese na razmerje med kakovostjo in ceno, **Iiyama** ponosno stopi v ospredje.

Poleg omenjenih proizvajalcev velja izpostaviti tudi **Hikvision**, ki svojo ponudbo dopolnjuje z interaktivnimi zasloni za poslovna in izobraževalna okolja. Zasloni z ločljivostjo 4K, podporo za večtočkovni dotik in vgrajenim operacijskim sistemom omogočajo enostavno sodelovanje, pisanje ter deljenje vsebin, zato so odlična izbira za sodobne učilnice in sejne sobe.

BenQ je že vrsto let uveljavljen proizvajalec projektorjev, monitorjev in interaktivnih zaslonov. Njihovi projektorji zagotavljajo kakovosten prikaz slike, dolgo življenjsko dobo svetlobnega vira in zanesljivo delovanje, zato so primerni tako za poslovno uporabo kot tudi za izobraževalne ustanove.

Sharp pa je sinonim za profesionalne projektorske rešitve. Njihova ponudba obsega zmogljive laserske projektorje za učilnice, sejne sobe in večje prireditvene prostore, poleg tega pa ponujajo tudi profesionalne zaslone, videostene in rešitve za digitalno prikazovanje vsebin. Zaradi vrhunske kakovosti slike in zanesljivega delovanja sodijo med vodilne proizvajalce avdiovizualne opreme.

Videokonferenca? Ni problema

Če želite opremiti sobo za videokonferenco, omenjeni proizvajalci ponujajo širok nabor rešitev, ki poleg zaslonov vključujejo tudi kamere, mikrofone ter sisteme za konferenco vse v enem (all-in-one conference bar).

Na voljo so različne možnosti – od kamer, nameščenih na zaslonih, do panoramskih kamer za celoten prostor ali naprednih sistemov, ki zaznavajo obraze, samodejno približajo in oddalijo govorca ter prilagodijo prikaz poteka sestanka. Takšne rešitve omogočajo, da se uporabniki osredotočijo na vsebino sestanka, tehnologija pa poskrbi za nemoteno delovanje.

Poleg tega posamezni proizvajalci ponujajo tudi celovite videokonferenčne sisteme za učilnice in sejne sobe, ki vključujejo interaktivne zaslone, kamere, slušalke in drugo AV-opremo. Rešitve so pogosto prilagojene za platforme, kot sta Microsoft Teams in Zoom, kar omogoča enostavno integracijo v obstoječa delovna okolja. (P.R.)

Acord-92 d.o.o.,
Stegne 13, 1000 Ljubljana
Tel.: +386 (0)1 583 72 30
brezplačna tel. št.: 080 26 29
e-pošta: info@acord-92.si
www.acord-92.si
www.pcplus.si

GO-LIX D.O.O.

Največja kibernetska grožnja sedi v vaši pisarni. Rešitev pa tudi

Slovensko podjetje GO-LIX je razvilo platformo Phishstrike, ki zaposlene ne kaznuje zaradi klika na napačno povezavo – ampak jih nauči, da ga naslednjič ne naredijo.

Ena najbolj nezaželenih besednih zvez v vsakem podjetju je kibernetski napad. Tehnična zaščita informacijskih sistemov, požarni zidovi, protivirusne rešitve … vse lepo in prav, a večina uspešnih vdorov se začne zaradi človeške napake.

Slovenska platforma za dvig varnostne kulture podjetij – Phishstrike

GO-LIX d.o.o. sodi med vodilna slovenska podjetja na področju red teaminga, sistemskih varnostnih pregledov, penetracijskega testiranja in digitalne forenzike. Dolgoletne izkušnje iz prakse so jih pripeljale tudi do razvoja lastne **slovenske platforme** za dvig varnostne kulture organizacij – Phishstrike.

Rešitev za podjetja vseh velikosti

Platforma je namenjena organizacijam in podjetjem, ki želijo sistematično izboljšati znanje zaposlenih in hkrati izpolnjevati zahteve zakonodaje, med drugim tudi **zakona ZInfV-1**. Na voljo je več različnih paketov, prilagojenih potrebam posameznih podjetij. Večjim organizacijam je namenjena celovita platforma za dvig varnostne kulture, manjša podjetja pa se lahko odločijo za izobraževalni modul, ki **celoletno izobražuje** vaše zaposlene.

Posebej so se specializirali tudi za izvedbo naprednih in ciljno usmerjenih **Phishing testiranj**, ki jih uspešno ponujajo na trgu. Stranke se lahko odločijo le za enkratno phishing izvedbo, paketno ali celoletno. Z lastnim razvojem ugodijo zahtevam še tako zahtevnih strank.

Ocenjevanje, testiranje in ciljno izobraževanje

Phishstrike temelji na preprostem, a izjemno učinkovitem načelu: zaposleni so lahko najšibkejši ali pa najmočnejši člen varnostne verige podjetja. Ker napadalci danes ciljajo predvsem na ljudi in ne več le na informacijske sisteme, postaja ozaveščanje zaposlenih ena ključnih naložb v varnost organizacije.

Platforma deluje po treh medsebojno povezanih korakih. Najprej **oceni** trenutno raven znanja posameznika in podjetju pokaže stopnjo varnostne kulture. Nato **preverja** njegovo odzivanje s simulacijami phishing napadov, na koncu pa ga **ciljno izobražuje** na področjih, kjer potrebuje največ dodatnega znanja. Takšen pristop omogoča bistveno boljše rezultate kot klasična enkratna izobraževanja, saj se vsebine prilagajajo dejanskim potrebam posameznika.

Posebna prednost platforme je, da simulira realne phishing napade in scenarije socialnega inženiringa, s katerimi preverja, kako bi se zaposleni odzvali v resnični situaciji. Na podlagi rezultatov podjetje pridobi **jasen vpogled** v vedenjske vzorce zaposlenih, področja največjih tveganj in njihov napredek skozi čas.

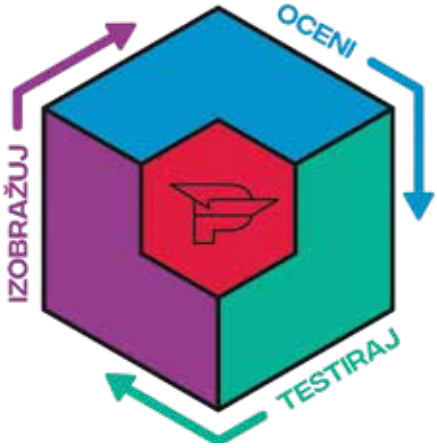
Prilagojena uporabniška izkušnja

Velik poudarek namenjajo tudi uporabniški izkušnji. Vsa izobraževanja potekajo v slovenskem jeziku (za slovenski trg), podpirajo pa tudi druge jezike, kot sta angleščina in hrvaščina. Zaposleni vsebine prejemajo neposredno po elektronski pošti (brez dodatnih prijav v sistem), čas za učenje pa si razporejajo sami glede na delovne obveznosti. Vsako izobraževanje se zaključi s kratkim kvizom, ki pomaga utrditi pridobljeno znanje. Po uspešno opravljenem programu zaposleni prejmejo tudi **potrdilo o izobraževanju**.

Platforma hkrati močno **razbremeni interne kadre**. Administratorji iz vrst IT-ja, kadrovska služba in vodstvo imajo na voljo pregledno **nadzorno ploščo** z vpogledom v potek izobraževanj, rezultate phishing testiranj, statistiko, poročila ter upravljanje uporabnikov.

Vsebine sledijo aktualnim grožnjam

Izobraževalne vsebine pripravljajo strokovnjaki za kibernetsko varnost in jih redno posodabljajo glede na aktualne grožnje. Program je razdeljen na dva sklopa. Obvezni del temelji na priporočilih Urada Vlade Republike Slovenije za informacijsko varnost in zajema vsebine, potrebne za osnovno usposabljanje s področja informacijske in kibernetske varnosti. Dodatni sklop pa obravnava vsakodnevne teme, kot so prepoznavanje lažnih domen in poddomen, varna uporaba gesel, nevarnosti spleta, varna uporaba USB-ključkov, informacijska varnost ter številna druga področja, s katerimi se zaposleni srečujejo pri vsakodnevnem delu.



Dolgoročna naložba v varnejše poslovanje

Phishstrike ne temelji na kaznovanju napak, ampak na pozitivni motivaciji. Zaposlene spodbuja k razmišljanju o spletnih prevarah in postopno gradi kulturo odgovornega ravnanja. Prav ponavljanje procesa ocenjevanja, testiranja in izobraževanja skozi vse leto zagotavlja dolgoročne rezultate ter bistveno zmanjša možnost uspešnih kibernetskih napadov.

Tehnologija sama ni dovolj, največjo razliko naredijo ljudje.

Več lahko najdete na www.phishstrike.com. (P.R.)

GO-LIX,
kibernetska in informacijska varnost d.o.o.

GO-LIX

Cesta Goriške fronte 46
5290 Šempeter pri Gorici
info@golix.si
www.golix.si

Granblue Fantasy: Relink – Endless Ragnarok

Datum izida: 9. julij
Platforme: Nintendo Switch 2, PlayStation 5

Granblue Fantasy: Relink – Endless Ragnarok je obsežna samostojna razširitev priljubljenega akcijskega RPG-ja, ki nadaljuje zgodbo po dogodkih iz izvirne igre. Igralci se znova podajo na epsko pustolovščino po lebdečih otokih sveta Sky Realm, kjer jih čakajo novi sovražniki, mogočni šefi in nova zgodba. Razširitev prinaša dodatne igrive like, zahtevnejše kooperativne misije, novo stopnjo Chaos Quest ter izboljšave sistema napredovanja. Novost je tudi način Conflux za samostojno igranje ter možnost uporabe mogočnih priklicev v boju. Igra prvič podpira popoln crossplay med vsemi platformami, zato lahko igralci sodelujejo ne glede na izbrano napravo. Endless Ragnarok predstavlja največjo vsebinsko nadgradnjo igre doslej in ponuja več deset ur nove akcije za veterane ter odlično izhodišče tudi za nove igralce.

MOUSE: P.I. For Hire

Datum izida: 10. julij
Platforme: PlayStation 5, Xbox Series X, PC

MOUSE: P.I. For Hire je edinstvena prvoosebna akcijska igra, ki združuje hitro FPS-igranje z detektivsko zgodbo v slogu noir filmov. Dogajanje je postavljeno v mesto Mouseburg, kjer igralci prevzamejo vlogo zasebnega detektiva Jacka Pepperja in raziskujejo zarote, kriminal ter korupcijo. Posebnost igre je vizualna podoba, navdihnjena z ročno risanimi risankami iz 30. let prejšnjega stoletja, ki ustvarja prepoznaven črno-bel slog z izrazito filmskim vzdušjem. Poleg intenzivnih strelskih obračunov igra vključuje raziskovanje, zbiranje dokazov, reševanje ugank in uporabo različnih pripomočkov. Številne skrivnosti, nadgradnje orožij in razgibane stopnje poskrbijo za pestro igranje, ki združuje nostalgijo klasičnih "boomer shooterjev" z modernimi igralnimi mehanikami in humorjem.

Beast of Reincarnation

Datum izida: 4. avgust
Platforme: PlayStation 5, Xbox Series X

Beast of Reincarnation je akcijski RPG studia Game Freak, ki igralce popelje v postapokaliptično Japonsko leta 4026. V ospredju zgodbe sta mlada bojevnica Emma in njen zvesti pasji spremljevalec Koo, ki skupaj raziskujeta svet, uničen zaradi skrivnostne pokvarjenosti narave. Bojni sistem temelji na hitrih in tehnično zahtevnih spopadih, pri katerih je ključno usklajeno sodelovanje med Emmo in Koojem. Med raziskovanjem igralci odkrivajo opuščena mesta, gozdove in ruševine, premagujejo ogromne zveri ter mehanske nasprotnike in postopoma razkrivajo skrivnost propada sveta. Igra navdušuje z vizualno dovršeno podobo, čustveno zgodbo in poudarkom na raziskovanju ter razvoju sposobnosti obeh glavnih junakov. Gre za prvo veliko izvirno akcijsko RPG-igro studia Game Freak zunaj franšize Pokémon.

mali OGLASI | Računalniške novice

www.racunalniske-novice.com

KUPUJETE ALI PRODAJATE RAČUNALNIŠKO OPREMO?

Oddajte svoj brezplačni oglas na www.racunalniske-novice.com/mali-oglasi

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 €**

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 €**

Slušalke športne Philips TAA5508

Brezžične športne slušalke z odpravljanjem šumov. Malo uporabljene. Različni nastavki za ušesa. Lahko pošljem po pošti. **60,00 €**

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 €**

Samsung E2121B

Samsung E2121B, ohranjen in brezhibno delujoč z originalnim polnilcem. Je odklenjen na vse SIM kartice. **30,00 €**

Thermalright Burst Assassin 120 ARGB

Prodam 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 €**

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 z 32 GB RAM-a in 1 TB SSD diskom ... **1.799,00 €**

Prodam 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 €**

AirPods 4

Prodam 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 €**

Gaming PC Microstar intel i5,

8GB RAM, Nvidia GTX 1050 Ti 4GB, SSD, prodam Gaming PC Microstar (MSI) sestavljen iz sledečih komponent:
Osnovna plošča: MSI MS-7728 H61 **160,00 €**

Barvni laserski tiskalnik, Samsung

Prodam multifunkcijski Samsung CLX-6260FW z napako. barvni tiskalnik, ločljivost tiskanja: do 9600 × 600 dpi, hitrost tiskanja: do 24 str/min (barvno), hitrost ... **250,00 €**

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 €**

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 €**

INTEL procesor za prenosni računalnik

- 1.80/2M/800
- LF80537T7100
- FRU 42W7654
- SLA4A
- Odlično ohranjen in delujoč, ... **15,00 €**

ASUS grafična kartica

Dual Radeon RX 580 O 8GB.
Prodam ASUS grafična kartica Dual Radeon RX 580 O 8GB . Imam več komadov (8 kom.). Če kupiš vse dam količinski popust. **100,00 €**

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 €**

Električni skiro Manta

Prodaja se lepo ohranjen električni skiro star 2leti malo vožen. Z enim polnjenjem se naredi do 40 km, 25 KM/H, DO 120 KG PREVZEM MB. **300,00 €**

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 €**

Napajalnik Dell 685W 80+ Gold

H685EF-00 za strežnike/delovne postaje. Brezhiben, primeren za strežnike/delovne postaje serij Dell Precision T5610, T5810, T7810, T7910,... **50,00 €**

ASUS PRIME Z370-P Motherboard

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

Polaroid Land Camera 1000

Prodam vintage Polaroid Land Camera 1000 retro instant fotoaparat. Aparat je lepo ohranjen, normalen znak uporabe glede na starost, brez razpok ali poškodb ... **70,00 €**

Segway, P65 Električni skiro

Praktično nov, odprta embalaža.
Ni vožen / brez poškodb.
Močan motor, doseg do 65 km.
Trgovinska cena 900€+. **649,99 €**

SSD SAMSUNG 860 PRO 256 GB SATA3

Prodam nov zapakiran SSD, SAMSUNG 860 PRO 256 GB, 2.5", SATA3, V-NAND, MLC, 7 mm. **40,00 €**

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 €**

Asus K55VJ Intel i7, 8GB RAM,

USB mikrofon z zelo dobrim studijskim zvokom, primeren za streaming, gaming, podcast ali ustvarjanje vsebin. Deluje brezhibno, priložen je original kabel ... **119,99 €**

Gaming računalnik i7

16 GB RAM / GTX 1070 / 756GB SSD / 4TB HDD. Prodam na novo sestavljen in popolnoma očiščen gaming računalnik. Sveža namestitev Windows 10 Pro (aktivirani) ... **229,00 €**

Xiaomi 15 Ultra, 512 GB, 16 GB RAM

Prodam vrhunsko ohranjen telefon (6,73-palčni) jasen zaslon z ločljivostjo 3200 × 1440 pik, AMOLED WQHD+, frekvenca osveževanja 120 Hz, 68 bilijonov barv, HDR10+ ... **940,00 €**

Prodam Philips LED monitor

18 palični Philips LED monitor 197E, ki ga odlikujeta odlična kakovost slike in eleganten izgled. Ločljivost 1366 x 768, TFT zaslonska plošča, format, ... **40,00 €**

Nokia N97 - 4 Mini RM-555

Redek model, odklenjen na vse sim kartice, priložen originalni polnilec. **90,00 €**

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 €**

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 €**

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 €**

Samsung s25 Ultra 512GB

Prodam samsung s25 Ultra s 512GB spomina. Star je cca. 6mesecev (v uporabi je bil samo slab mesec), in je dobro ohranjen. Nameščeno ima zaščitno steklo, ... **969,00 €**

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 €**

Instax mini 11 – instant fotoaparat

Kamera je lepo ohranjena, malo uporabljena in deluje brezhibno. Uporablja Instax Mini film. Ima samodejno prilagajanje osvetlitve, selfie način in vgrajeno bliskavico. **60,00 €**

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 €**

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 €**

Lenovo ThinkPad L470

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

Objavljeni oglasi so bili aktualni ob pripravi revije.

Za ogled najnovejših ponudb skeniraj QR kodo.

Oglasi niso lektorirani.

Odprtokodna orodja, ki lahko zamenjajo znane in drage rešitve

Vsake toliko časa naletim na program, pri katerem se vprašam, zakaj ga ne uporablja več ljudi?

Včasih je to majhno orodje za pošiljanje datotek. Drugič je celoten pogon za razvoj iger, sistem za samogostovanje aplikacij, urejevalnik zvoka ali program za analizo omrežja, s katerim lahko točno vidiš, kaj se dogaja v tvojem omrežju.

Odprtokodna programska oprema ima pri nekaterih uporabnikih čuden sloves. Nekateri jo še vedno razumejo kot brezplačen nadomestek, ki je uporaben samo, če nimaš denarja za »pravi« program. To je zastarel pogled. Danes so nekateri odprtokodni projekti boljši, bolj pregledni in bolj pošteni od zaprtih alternativ. Ne vedno. Odprtokodno ne pomeni samodejno boljše. Pomeni pa, da je izvorna koda dostopna, da jo lahko skupnost preverja, popravlja, prilagaja in razvija naprej. Pri nekaterih projektih je to tudi zaščita pred tem, da bi uporabnik čez noč postal ujetnik ene storitve, ene naročnine ali ene poslovne odločitve.

LocalSend je za lokalno pošiljanje, AlterSend pa za vse ostalo

AlterSend je orodje za neposredno pošiljanje datotek med napravami. Ideja je zelo preprosta. Napravi se povežeta, običajno prek QR kode, datoteka pa potuje neposredno med njima, šifrirano in brez nalaganja v oblak. To pomeni brez računa, brez omejitve velikosti v smislu klasičnih spletnih rešitev in brez vprašanja, kje je datoteka dejansko pristala. Nadomesti lahko WeTransfer, Dropbox Transfer, Google Drive povezave ali razne spletne strani za pošiljanje datotek. Seveda to ni isto kot dolgoročna shramba v oblaku. Če želite arhiv, deljenje map in zgodovino različic, boste še vedno uporabili Nextcloud, Google Drive ali Dropbox. Če pa želite prijatelju, sodelavcu ali sebi na drugo napravo poslati veliko datoteko brez posrednika, je AlterSend dober odgovor.

Če bi radi sebi poslali datoteko, na primer iz računalnika na telefon, lahko uporabite LocalSend. Princip je zelo podoben, vendar izmenjava deluje samo za naprave, ki so v istem omrežju.

NetBird je VPN za ljudi, ki ne želijo izvajati vragolij z omrežjem

NetBird je odprtokodna rešitev za varno povezovanje računalnikov, strežnikov, NAS-ov in oddaljenih uporabnikov v zasebno omrežje. V ozadju uporablja WireGuard, vendar mu doda preprostejše upravljanje naprav, uporabnikov in pravil dostopa. Namesto da na usmerjevalniku odpiramo porte, nastavljamo DDNS in upamo, da nismo po nesreči izpostavili polovice domačega omrežja internetu, na naprave namestimo odjemalca in jih povežemo skozi šifrirano zasebno povezavo.

Pristop Zero Trust pomeni, da dostop ni samoumeven. Uporabnik ali naprava vidi samo tisto, kar ji dovolimo. Zato je NetBird odlična alternativa klasičnemu VPN-ju, OpenVPN-ju, ZeroTierju ali Tailscalu – predvsem za domače strežnike, NAS, interne aplikacije in manjša podjetja.

Wireshark vidi skoraj vse

Wireshark je orodje za analizo omrežnih protokolov. Z njim zajamemo promet in vidimo pakete, protokole, naslove, vrata, DNS poizvedbe, TCP povezave in veliko drugih podrobnosti. Wireshark je lahko zelo močno orodje, da se poglobimo v naše omrežje in ugotovimo, kaj se sploh dogaja v optičnih kablih in brezžičnih valovih.

Nadomesti lahko del uporabe tcpdumpa, komercialnih analizatorjev prometa in veliko slepega ugibanja pri omrežnih težavah. Ni orodje za začetnika, ki želi preveriti le hitrost interneta. Je pa neprecenljivo, ko morate ugotoviti, ali težava nastane pri DNS-u, povezavi, TLS-u, aplikaciji ali strežniku.

FFmpeg je švicarski nož za zvok in video

FFmpeg je eno tistih orodij, ki ga veliko ljudi uporablja, tudi če tega ne ve. V ozadju ga uporabljajo številni programi in storitve, ker zna pretvarjati, rezati, združevati, snemati, stiskati in pretakati skoraj vse, kar je povezano z zvokom in videom.

Lahko nadomesti različne video konverterje, spletne pretvornike, del funkcij Adobe Media Encoderja, HandBrake v bolj tehničnih scenarijih in kup majhnih programov, ki znajo samo eno stvar. FFmpeg je ukaznovrstično orodje, kar pomeni, da na začetku deluje malo surovo. Ko pa ga enkrat usvojiš, postane zelo uporaben.

Iz videa lahko na primer v nekaj sekundah izlu-

ščiš zvok, zmanjšaš velikost posnetka, pretvoriš format, odrežeš začetek in konec ali pripraviš datoteko za spletno objavo.

Darktable je kot fotografska temnica

Darktable je odprtokodni program za fotografski potek dela in razvijanje RAW datotek. Najlažje ga razumemo kot alternativo Adobe Lightroomu. Upravlja fotografsko knjižnico, omogoča nedestruktivno obdelavo RAW posnetkov in izvoz končnih fotografij.

Nedestruktivno pomeni, da izvirne datoteke ne uničujemo. Program si zapomni korake obdelave, fotografija pa ostane izvirna.

Darktable ni najlažji program za začetnika, ker ima veliko modulov in drugačno logiko kot Lightroom. A ko razumeš maske, osvetlitev, barvno korekcijo in lokalne prilagoditve, postane veliko bolj razumljiv. Moj nasvet bi bil, da ne poskušajte kar takoj uporabljati vseh modulov. Izberite nekaj osnovnih in jih usvojite. Pri fotografiji preveč drsnikov hitro naredi več škode kot koristi.

Coolify je uporaben v rokah razvijalcev

Coolify je samogostovana odprtokodna PaaS rešitev. To pomeni, da na lastnem strežniku dobiš izkušnjo, kot jo ponujajo Heroku, Vercel, Netlify ali Railway. Namesto da ročno nastavljaš Docker, reverse proxy, SSL certifikate in okoljske spremenljivke za vsako aplikacijo posebej, Coolify veliko tega poenostavi v spletnem vmesniku.

Zelo uporaben je za razvijalce, ki imajo VPS in želijo na njem poganjati spletne strani, API-je, baze podatkov, WordPress, Ghost, Plausible, Uptime Kuma ali druge storitve. Coolify je odličen za manjše produkcijske projekte in interne storitve, ga pa ne bi brez premisleka postavil kot edini temelj za kritično infrastrukturo brez varnostnih kopij in nadzora.

PostgreSQL: baza, ki jo prerasteš težje kot večino drugih

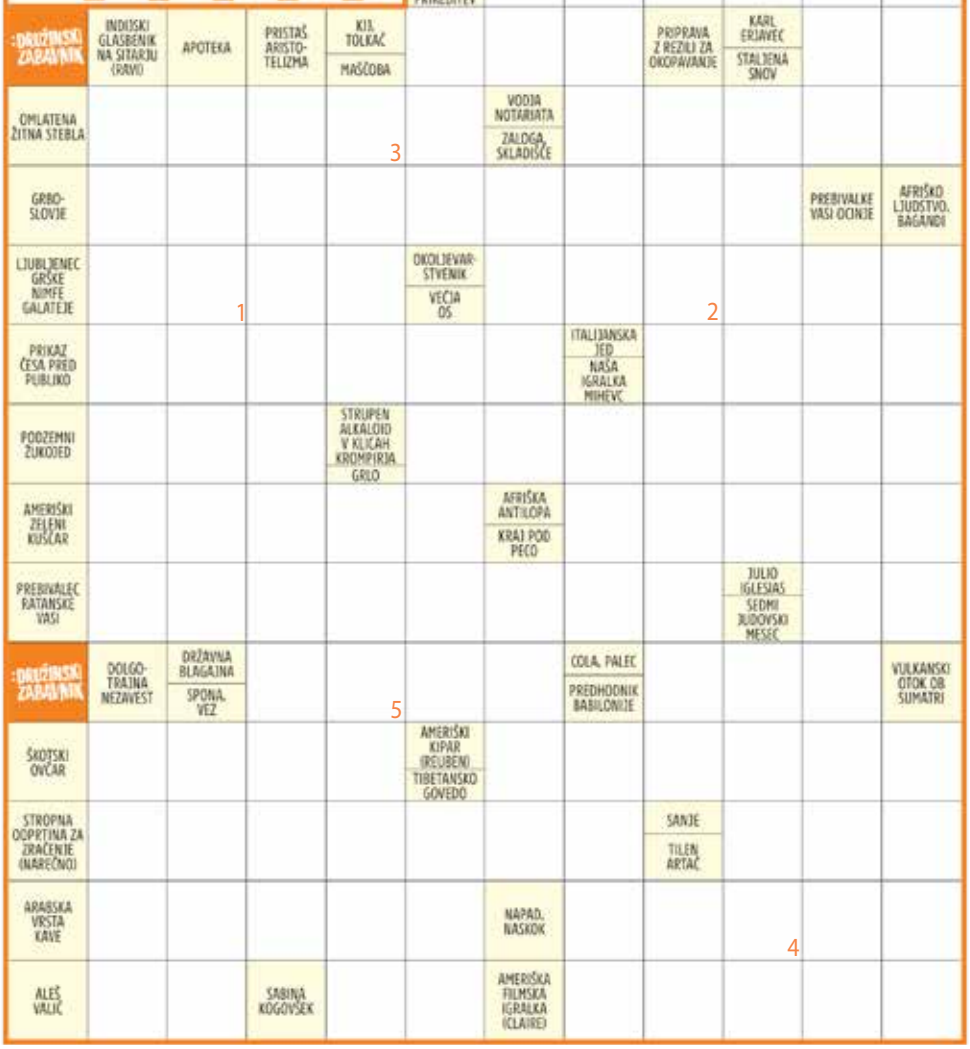
PostgreSQL niti ni alternativa nobenemu programu. Beseda je skoraj žaljiva za takšno storitev. Ni samo brezplačna zamenjava za MySQL ali cenejša pot okoli komercialnih baz. PostgreSQL je resna objektno-relacijska podatkovna baza, ki jo uporabljajo majhni projekti, zagonska podjetja, spletne storitve, analitični sistemi in velika poslovna okolja. Obvlada klasični SQL, transakcije, kompleksne poizvedbe, napredne indekse, JSON, razširitve in s PostGIS dodatkom tudi zelo zmogljivo delo z geografskimi podatki.

Njena prednost je, da raste skupaj s projektom. Začneš lahko z majhno aplikacijo, potem dodaš več tabel, več uporabnikov, več podatkov, bolj zapletene poizvedbe, API-je, poročila, geografske sloje in analitiko, PostgreSQL pa se ne začne takoj pritoževati. Slabo zasnovana baza bo počasna tudi v PostgreSQL-u. Razlika je v tem, da imaš na voljo zelo veliko orodij, da težavo rešiš pravilno.

Odprtokodni programi so zelo pomembna protiutež

Odprtokodnost ni religija in tudi ni garancija, da bo program boljši. Je pa zelo pomembna protiutež svetu, v katerem se skoraj vse spreminja v naročnino, oblak in zaklenjen ekosistem. Pri odprtokodnih orodjih ima uporabnik pogosto več nadzora. Lahko jih uporablja brez prisile v določen poslovni model, lahko jih gosti sam, lahko preveri, kako delujejo, in lahko jih skupnost razvija še dolgo po tem, ko bi komercialni izdelek morda že ukinili.

Niso vsi programi za vsakogar. In prav je tako. Ampak če vsaj enega od njih dodate v svoj delovni tok, boste presenečeni, na kakšno orodje ste naleteli čisto spotoma.



VAGANT: potujoči srednjeveški sholar, **SOLANIN:** strupen alkaloid, **NAKIAN:** am. kipar, **GANDI:** afr. ljudstvo, **LARINKS:** grlo

NAGRADE in NAGRAJENCI

Med reševalce, ki bodo do petka, **28. 8. 2026**, poslali pravilno rešitev, bomo z žrebom razdelili privlačne nagrade:

3x PowerBank Joyroom JR-PBF12

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

Bluetooth slušalke Joyroom ANC JR-FN3 prejmejo:

- **Milan Metelko, Studenec**
- **Štefan Pavovec, Domžale**
- **Davor Tavčar, Škofja Loka**
- **Drago Lipič, Sveta Trojica v Slov. Gor.**

Nagrade podarja podjetje Stromboli, d.o.o.

Rešitev križanke 11/XXXI: BALON

KOLEDAR DOGODKOV

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

Naročnine:
tel.: 01 / 620 88 00,
narocnine@stromboli.si

Oglasno trženje:
Matej Komprej, tel.: 01 / 620 88 06
gsm: 070 / 606 152, matej.komprej@stromboli.si

Boštjan Štrukelj, tel.: 01 / 620 88 01,
gsm: 041 / 663 301, bostjan.strukelj@stromboli.si

Ana Kopitar, tel.: 01 / 620 88 09,
ana.kopitar@stromboli.si

Sodelavci in novinarji:
Maja Lavrač, Matej Saksida, Peter Čebron
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

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 Predstavitev in na koncu članka s (P.R.) – Payable Release (plačani članek) – pripravljamo v sodelovanju s podjetji.

Sporočila za javnost sprejemamo na Rn@stromboli.si. Izid revije je finančno podprla Javna agencija za raziskovalno dejavnost Republike Slovenije.

InterMAC, d.o.o., Kranj, Golniška c. 43, SI-4000 Kranj Tel.: (04) 20 47 340, Fax: (04) 20 47 345, E-mail: info@kupisi.net

Prenosni Računalnik

HP EliteBook 8 G1a 16

Najuspešnejšim ekipam zagotovite računalnik, izboljšan z umetno inteligenco, ki zagotavlja zmogljivost, varnost in orodja za sodelovanje, ki so bistvena za pisarniška in hibridna delovna okolja. Računalnik HP EliteBook 8 G1a z diagonalo zaslona 16 palcev učinkovito izpolnjuje zahteve večopravilnih skupin po vsem svetu.

- **Procesor AMD Ryzen™ 5 230 (3,5 - 4,9 GHz) 16MB 6C/12T**
- Windows 11 Pro 64 bit, SLO ali ANG
- 40,64 cm (16") WUXGA sRGB 62,5%, 1920x1200, nebleščeč 300 nitni
- Grafična kartica integrirana AMD Radeon™ Grphics
- 16 GB DDR5 5600 MHz (1 x 16 GB), ena prosta reža, do 64GB
- 512 GB PCIe® NVMe™ Value
- 2x USB-C® (Tunderbolt™ 4), 1x HDMI 2.1, 1x USB A 5Gbps, 1x RJ-45
- Mediatek RZ616 Wi-Fi 6E +BT 5.3 WW
- Kombiniran stereo izhod/mikrofon vhod
- Zvok Poly Studio, 2 vgrajena zvočnika in mikrofona, kamera 5 MP
- TPM 2.0 modul, reža za varnostno ključavnico, bralnik prstnih odtisov
- Osvetljena SLO tipkovnica HP Premium Durakey, odporna proti razlitju, ločena številčnica
- Garancija 3 leta (tudi baterija, 62Wh, 3 celična Li-Ion, HP Slim 100W USB-C® adapter)

AD4J1ET

Cena: 1.889,00 z DDV

HP EliteBook G1i 16 z AMD Ryzen™ 5 230 procesorjem in AMD Radeon™ Graphics

InterMAC, d.o.o., Kranj, Golniška c. 43, SI-4000 Kranj Tel.: (04) 20 47 340, Fax: (04) 20 47 345, E-mail: info@kupisi.net

iStor.

Data Protection. Done Properly. Since 1999.

Pri iStoru **varnostno shranjevanje podatkov** ni le gola funkcija – je disciplina. Že več kot četrt stoletja zagotavljamo eno najvarnejših celovitih storitev **varnostnega shranjevanja podatkov** v Evropi.

VARNOSTNO SHRANJEVANJE PODATKOV

Oddaljeno shranjevanje (Off-site)

Izolirane varnostne kopije (Off-line)

Varnostne kopije z EMP zaščito

DOLGOROČNO ARHIVIRANJE E-POŠTE

DNK ARHIVIRANJE

iStor d.o.o. | 059 74 11 50 | info@istor.si | www.istor.si