Računalniške novice

Cena: 1,99 €

Kako prepoznati spletne goljufije?

št. 6/XXIX
28. marec 2024

Kibernetska varnost je ključavnica, ključ je v vaših rokah

» Na testu polnilna postaja BLUETTI AC180 - ni me razočarala

» TikTok še korak bližje popolni blokadi v ZDA

» Negativen vpliv umetne inteligence in robotov

Digitalni LED pingvini: novi trend v vizualnih prikazih

Moč in prilagodljivost podatkovnih sistemov Lenovo

Varno in učinkovito IT upravljanje

Vrhunska varnost s kamerami, senzorji, kontrolo pristopa …


33.
SOF
SLOVENSKI OGLAŠEVALSKI FESTIVAL
USTVARJAMO
IN SLAVIMO
PRESEŽKE
6. – 7. JUNIJ 2024
AVDITORIJ PORTOROŽ

Microsoft Copilot: model GPT-4 Turbo odslej tudi brezplačno

Microsoft je razkril, da bo njihov Copilot deležen velike nagradnje: integracije z OpenAI-jevim modelom GPT-4 Turbo. Najboljše pri vsem tem pa je, da bodo imeli poln dostop do GPT-4 Turbo tudi brezplačni uporabniki.

Glede na objavo na družbenem omrežju X bodo imeli Pro uporabniki to prednost, da bodo lahko izbirali med GPT-4 Turbo in starejšim modelom GPT-4, ki je za specifične načine uporabe še vedno boljša možnost. Na tak način bo Microsoft uporabnikom, ki bodo imeli plačljivo verzijo, ponudil dodatne možnosti, ne da bi prikrajšal brezplačne uporabnike.

GPT-4 Turbo je izboljšana različica osnovnega modela GPT-4 in je dobro poznana po svoji hitrosti, natančnosti in zmožnosti upravljanja daljših, bolj kompleksnih opravil. Microsoftova posodobitev prinaša hitrejšo generacijo kode, bolj poglobljene rezultate in izboljšano odzivnost. Vse to bi naj privedlo do večje produktivnosti in bolj čistega procesa kodiranja.

Lepo je videti, da tudi uporabniki z brezplačno verzijo prejemajo pomembne posodobitve svojega AI pomočnika Copilot – vsekakor je pozitivno, da bo Microsoft zagotovil, da lahko vsi uporabniki, ne glede na finančne zmožnosti, še vedno koristijo njihovo storitev. To je pomembno tudi za Microsoft, ki se trudi pridobiti več uporabnikov na stran operacijskega sistema Windows 11, ki bo ponujal polno različico Copilota. Na drugi strani pa tudi Pro naročniki niso ostali praznih rok, saj jim posodobitev zagotavlja večjo prilagodljivost, ko gre za nadgradnje jezikovnega modela. Da ne omenjamo drugih funkcij in orodij, ki so bila doslej dodana.

Microsoft je pred kratkim napovedal novost, ki sliši na ime Copilot Chatbot in Pro uporabnikom omogoča ustvarjanje klepetalnih botov po meri. Ti so prilagojeni za posamezna opravila, na primer glede na vlogo uporabnika v profesionalnem življenju. Te posodobitve se je Microsoft lotil brez kakršnih koli prispevkov OpenAI-ja, kar lahko kaže na to, da se Microsoft počasi oddaljuje od tega podjetja, verjetno predvsem zaradi povečanega nadzora in tožb, s katerimi se ukvarjajo. Je pa to hkrati nenavadno, če upoštevamo, da je bila najnovejša posodobitev GPT dodana v Copilot.

Obstaja tudi funkcija, ki Copilotu omogoča neposredno branje datotek v računalniku. Uporabnik lahko tako dobi povzetek dokumenta, poišče določene podatke ali išče dodatne informacije na internetu. Kot vse kaže pa pri tem ne bo težav z vprašanjem zasebnosti, saj mora uporabnik datoteko ročno vstaviti v polje za Copilot klepet (ali izbrati možnost »Dodaj datoteko«) in nato uporabiti "prompt".

TikTok še korak bližje popolni blokadi v ZDA

Vsi dobro vemo, da je družbeno omrežje TikTok med uporabniki zelo priljubljeno. Ima že več kot dve milijardi prenosov na pametne mobilne telefone in tablične računalnike. TikTok je priljubljen predvsem zaradi kopice kratkih videoposnetkov, ki jih uporabniki hitro in enostavno objavijo, dodajajo učinke in raznovrstne digitalne filtre.

Nad njim pa že kar nekaj časa niso preveč navdušeni ameriški politiki, ki so prepričani, da omrežje nezakonito zbira osebne podatke ameriških uporabnikov. TikTok je že nekaj časa na zatožni klopi, direktor pa se je moral zagovarjati tudi pred ameriškimi senatorji. Pred kratkim pa je Predstavniški dom ameriškega kongresa z veliko večino podprl zakon za prepoved delovanja platforme TikTok na ameriških tleh. Ameriški senatorji so mnenja, da v ozadju platforme stoji kitajska vlada, ki med ameriško mladino širi propagando za spodkopavanje ameriške družbe.

Nov zakon mora podpisati še senat in predsednik Združenih držav Amerike. Če bo "zakon o zaščiti Američanov pred nadzorovanimi aplikacijami tujih podjetij" potrdil tako senat kot ameriški predsednik, bodo družbenemu omrežju pisane ure, podjetje ByteDance, ki upravlja s platformo TikTok, pa bo moralo v pol leta prodati ameriško izpostavo. Mnenja so deljena. Nekateri pravijo, da je to napad na svobodo govora, drugi pa podpirajo odločitev zaradi prevelikega nadzora tovrstnih platform nad osebnimi podatki uporabnikov. Kaj se bo zgodilo, bomo videli v naslednjih tednih.

ASUS Zenfone 11 Ultra: nedvomno vrhunski telefon

ASUS Zenfone je bila linija telefonov, ki je bila zadnji branik kompaktnih telefonov. Medtem ko večina proizvajalcev izdeluje telefone z diagonalo med 6,4 in 6,8 palcev, so bili Zenfone telefoni tudi manjši od 6 palcev, vseeno pa izredno zmogljivi in razmeroma poceni.

Najnovejši ASUS Zenfone 11 Ultra se s 6,78 palci požvižga na svoje poreklo. Ali to pomeni konec kompaktnih ASUS telefonov? Upamo, da ne, in da bomo v naslednjih mesecih dobili še navadne različice ASUS Zenfone 11 z manjšimi zasloni. Če odmislimo kompaktnost, je ASUS Zenfone 11 Ultra seveda odličen telefon. Sumljivo podoben je gaming telefonu ROG Phone 8, le da so mu odstranili vpadljivo RGB osvetljavo. Vgradili so čisto vse igračke, ki jih potrebujemo. Poganja ga najnovejši Snapdragon 8 Gen 3, ki smo ga že testirali v najnovejših Samsung in Xiaomi telefonih – in lahko rečemo, da ponuja zmogljivost, ki jo boste težko izkoristili v celoti. Sistemskega pomnilnika je 12 ali 16 GB, prostora za shranjevanje pa do 512 GB (hitri UFS 4.0).

Zaslon podpira LTPO tehnologijo za prilagajanje frekvence (1-144 Hz), najvišja je na voljo samo med igranjem iger, sicer pa lahko za vsakdanje naloge koristimo 120-Hz osveževanje. Glavna kamera se lahko pohvali z ločljivostjo 50 MP s solidno goriščnico f/1,9, na voljo pa sta še ultraširoka ločljivosti 13 MP in telefoto kamera (32 MP) s trikratno optično povečavo.

Samsung je z Galaxy S24 začel z vgradnjo AI funkcij, ostali mu sedaj sledijo. ASUS je vključil prevajanje v živo, ustvarjanje povzetkov iz zvočnih posnetkov, lažje iskanje fotografij ter ostalih elementov in globoko v nastavitvah bi se našlo še kaj. Cena osnovne različice je 899 evrov, z večjim pogonom pa 999 evrov, kar niti ni pretirano, še posebej, če telefon primerjamo z drugimi konkurenti.

Motorolina najnovejša telefona izgledata presenetljivo dobro

Nedavni nizkocenovni telefoni Motorola so bili zaradi pomanjkljivega dizajna, nesmiselnih dodatnih kamer in premajhnega nabora funkcij potisnjeni nekoliko v ozadje. Zdaj pa se zdi, da je na obzorju upanje: Moto G Power 5G in Moto G 5G 2024 izgledata precej dobro – vsaj na papirju.

Oba telefona končno ponujata NFC (zakaj tega ni bilo že od začetka, je uganka) in imata privlačno zadnjo stran iz veganskega usnja. Vključujeta tudi režo za kartico microSD in vgrajen vhod za slušalke, priročni funkciji, ki ju je večina proizvajalcev telefonov opustila že pred leti. G Power 5G prvič vključuje tudi brezžično polnjenje, ki je zelo redka funkcija pri katerem koli nizkocenovnem telefonu. Cena obeh modelov se začne pri 199 ameriških dolarjih (preračunanih 182 evrih) za Moto G 5G in 299 dolarjih (preračunanih 274 evrih) za Moto G Power 5G.

Dražji Moto G Power ima 6,7-palčni LCD zaslon ločljivosti 1080p s hitrostjo osveževanja 120 Hz – verjetno bi raje imeli OLED zaslon z večjim kontrastom in nižjo stopnjo osveževanja, toda za slabih 300 dolarjev si ne moremo preveč izmišljevati. Telefon uporablja nabor čipov srednjega razreda MediaTek Dimensity 7020 z 8 GB RAM-a, na zadnji strani pa sta samo dve kameri: glavna s 50 milijoni slikovnih pik z optično stabilizacijo in ultraširoka z 8 milijoni slikovnih pik s samodejnim ostrenjem, ki deluje tudi kot makro kamera. Poleg tega ni nobenih globinskih senzorjev z nizko ločljivostjo ali makro kamer, kot jih radi dodajajo ostali proizvajalci – pogosto se zdi, da samo zato, da lahko rečejo, da imajo več kamer kot konkurenca.

G Power podpira žično polnjenje z močjo do 30 W, vendar boste morali za to hitrost kupiti polnilec posebej. Podprto je tudi brezžično polnjenje (do 15 W). V napravi je ogromna baterija s 5000 mAh, isto pa ima tudi cenejši Moto G 5G.

Cenejši Moto G 5G poganja Qualcomm Snapdragon 4 Gen 1 s 4 GB RAM-a in vključuje 6,6-palčni LCD zaslon (ločljivosti 720p) s frekvenco osveževanja 120 Hz. Na voljo sta glavna kamera ločljivosti 50 MP in makro kamera z 2 MP. Žično polnjenje zmore največ 18 W, a če se vam pri polnjenje baterije ne bo posebej mudijo, bo to povsem dovolj. Tako kot G Power je ta model le »vodoodporen« in ni certificiran za popolno odpornost proti prahu ali potopitvi v vodo – žal, a pričakovano za proračunski razred, v katerem se nahajamo.

Kot vse kaže se na področju Motorolinih mobilnih naprav obetajo velike spremembe, a kot vedno je veliko odvisno od same izvedbe. Dejstvo pa je, da ne bo potrebno dolgo čakati, da izvemo, kaj prinašata oba telefona: Moto G Power je na voljo od 22. marca, mednarodna različica brez vezave pa od 29. marca dalje. Moto G 5G bo na voljo nekoliko kasneje.

E-bralnik Onyx Boox Note Air3 v Evropi

Onxy Boox Note Air3 je bil doslej bolj ali manj na voljo samo čez lužo. Evropski entuziasti bi lahko e-bralnik vseeno uvozili, vendar je s tem veliko dela in nihče se ne želi ukvarjati z garancijo s tujim podjetjem, še posebej ne na drugem koncu sveta. Odslej pa je ta dokaj nenavadni e-bralnik na voljo tudi v Evropi.

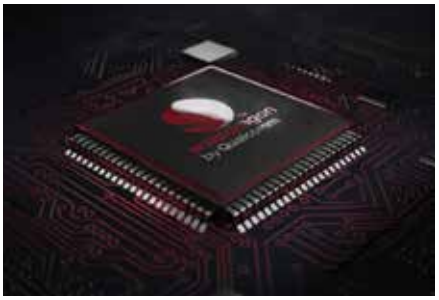
Novi Onyx Boox Note Air3 združuje prednosti klasičnih bralnikov elektronskih knjig s prednostmi tabličnih računalnikov. Je e-bralnik z nameščenim sistemom Android 12. To pomeni, da bi ga lahko v teoriji poleg branja e-knjig in stripov uporabljali tudi za druge naloge. Nanj lahko namestimo praktično katerokoli aplikacijo, ki jo najdemo v Google trgovini. Vprašanje pa je, kako se bo obnesla na e-ink zaslonu. Ti niso ravno najboljši medij za vsakdanje naloge, kot so na primer brskanje po spletu, gledanje posnetkov ali igranje iger. Zaslon ni tako hiter kot smo vajeni na primer na pametnem telefonu ali monitorju, kjer so animacije gladke in hitre. Tudi na splošno so e-bralniki počasnejši, ker za svojo primarno nalogo ne potrebujejo najmočnejših komponent.

Dober primer uporabe za novi Onyx Boox Note Air3 bi lahko bilo ustvarjanje dokumentov, grafov in podobnih elementov. Če še nikoli niste uporabljali e-ink zaslona, bo prva izkušnja zagotovo nenavadna, sčasoma pa boste ugotovili njegove prednosti. Onyx Boox Note Air3 podpira tudi uporabo pisala na 10,3-palčnem zaslonu, ki podpira ločljivosti do 1872 x 1404 slikovnih pik. Zaslon ima stekleno zaščito, ki bo preprečila prehitro obrabo. Tako kot pri skoraj vseh e-bralnikih, lahko tudi tukaj nadziramo temperaturo

barv in intenzivnost svetilnosti. Onyx Boox Note Air3 ima 4 GB RAM-a in 64 GB prostora za shranjevanje z možnostjo razširitve s kartico micro-SD. Cena se giblje okoli 400-450 evrov.

Snapdragon 8s Gen 3: cenejši, a skoraj enako zmogljiv

Qualcomm se v zadnjih letih s svojimi čipi ni prav veliko poigraval. Zadnje tri generacije je vedno popestril z modeli Plus (+), v zadnjem letu pa smo opazili še modele z dodatno oznako "s", kot na primer pri Snapdragon 7s Gen 2. Oznaka Plus označuje nekoliko hitrejša jedra,



morda podporo za večje konfiguracije RAM-a in podobno. Oznaka "s" pa pomeni, da gre za procesor, ki je ujet med prejšnjo in zdajšnjo generacijo. Ima lastnosti obeh, vprašanje je samo, koliksen del lastnosti so pobrali od novejšega procesorja. Snapdragon 8s Gen 3 je najnovejši tovrstni primerek, ki pa še ni bil vgrajen v noben telefon. To naj bi se zgodilo v prihodnjih mesecih, čeprav do takrat ni več nobenega večjega izida telefonov. Proti koncu poletja prihaja nova generacija zložljivih telefonov Samsung in Honor, v septembru pa nova generacija telefonov Xiaomi T. Slednja ima morda še največji potencial za vgradnjo teh novih čipov, saj gre za telefone visokega srednjega razreda, ki so prav tako ujeti med nižjim srednjim razredom (do nekje 500 evrov) in premijskim (nad 1000 evrov).

8s Gen 3 je 4-nm čip z glavnim jedrom Cortex-X4 pri 3,0 GHz, štirimi zmogljivimi jedri pri 2,8 GHz in tremi učinkovitimi jedri pri 2,0 GHz. Podpira do 24 GB pomnilnika LPDDR5x (do 4200 MHz) in pomnilnik UFS 4.0. Za povezljivost uporablja USB 3.1 Gen 2 prek USB-C. Sodeč po teh lastnostnih ne gre samo za okrnjeno različico najnovejšega Snapdragon 8 Gen 3 oziroma za porabo zalog čipov, ki niso ustrezali strogim standardom za novi čip, kar je spodbudno. Ima jedro Cortex-X4 z nižjim taktom, vendar tudi 4 velika jedra in 3 mala jedra v konfiguraciji 1+4+3. Originalni čip 8 Gen 3 je v konfiguraciji 1+5+2.

Podpora za RAM je bolj podobna lanskemu 8 Gen 2 in vgrajen je tudi starejši Snapdragon X70 5G modem (namesto X75). Vendar pa Qualcomm pravi, da 8s Gen 3 implementira 3GPP Release 17 in 5G varčevanje z energijo, česar ne najdemo pri starejšemu čipu. V vsakem primeru je čip pripravljen na novi standard Wi-Fi 7.

Dober bi moral biti tudi pri nalogah umetne inteligence. Ima vgrajen AI čip za tovrstne scenarije, česar nismo opazili pri Snapdragon 8 Gen 2. Zagotovo bo manj zmogljiv kot najnovejši čip, a vseeno dovolj hiter za zagon modelov Gemini, Llama 2 in podobnih.

Za igranje iger je Snapdragon 8s Gen 3 (SM8635) opremljen z zmogljivim grafičnim procesorjem Adreno 735. Podpira tudi strojno pospešeno sledenje žarkom (angl. ray tracing). Adreno Frame Motion Engine 2.0 lahko podvoji hitrost sličic na sekundo brez dodatne porabe energije, Snapdragon Game Super Resolution pa sliki brez dodatnih obremenitev doda pike.

Skratka, na papirju zelo soliden čip, ki ga bomo do konca letošnjega leta zagotovo testirali.

Gigabyte predstavil QD-OLED monitor

Tisti, ki spremljate področje monitorjev, ste zagotovo že slišali za QD-OLED panele. Dell je bil med prvimi, ki jih je pripeljal v razred 27-palčnih zaslonov in jim dodal še visoke hitrosti osveževanja (360 Hz). Cena kupcem ni bila prijazna, a prvi preizkuševalci nove tehnologije se na ceno skoraj vedno požvižgajo. Odtlej so se prebudili še ostali proizvajalci in cene tovrstnih monitorjev sedaj padajo. MSI je prejšnji mesec predstavil svojega kandidata, ki je za dobrega stotaka cenejši od Dellovega.

Sedaj je na vrsti Gigabyte. Gigabyte AORUS FO27Q3 (proizvajalci še vedno ne znajo dobro poimenovati monitorjev) uporablja Samsungovo panelo QD-OLED tretje generacije. Ločljivost je 1440p, frekvenca osveževanja pa tako kot pri podobnih modelih visokih 360 Hz. Če boste

sploh želeli doseči tovrstno frekvenco v igrah, boste potrebovali kar spodobno grafično kartico, in še to zgolj v igrah, kot so Doom Eternal, PUBG, Counter Strike in podobne. Odzivni čas je super kratek, okoli 0,03 milisekunde, povprečje pa bo zagotovo nekoliko višje.

Med priključki novega monitorja najdemo DisplayPort 1.4, VESA vmesnik za nosilce, 3,5-mm priključek za slušalke, USB Type-C, 2x HDMI 2.1, 3x USB 3.0. Podpira barvni razpon 99 % DCI-P3 in 10-bitne barve, če vam je to seveda sploh pomembno pri igranju iger. Za zaščito oči je integrirana tehnologija OLED care, ki zmanjša škodljivo modro svetlobo.

Največji ljubitelji računalniških iger ne prisegajo na kompromise. Še posebej pri stvareh, kot so računalniški zasloni. Večja kot je namreč frekvenca osveževanja zaslona in manjši kot je zakasnitveni čas, boljši je izid pri igranju računalniških iger. To je tudi glavni razlog, zakaj so se tudi pri podjetju Gigabyte odločili za pripravo po mnenju mnogih enega najboljših ukrivljenih računalniških zaslonov za sodobne in grafično bogate igre – Aorus FO27Q3. Novi Gigabyte Aorus FO27Q3 je na tujih trgih že na voljo. Njegova maloprodajna cena pa je pričakovano na nivoju konkurence, okoli 700-800 evrov.

Vzdržljiv telefon z dobrim zaslonom na voljo v Evropi

Podjetje Doogee je v evropskem prostoru nedavno ponudilo v prodajo enega izmed trenutno najzmogljivejših robustnih pametnih mobilnih telefonov. Telefon Doogee DK10 bo všeč izključno avanturistom, ki ne želijo, da se telefon poškoduje ob prvem stiku s tlemi. Novi Doogee ima celo kovinsko ohišje, ki je odporno na prah in vodo ter združljivo z vzdržljivostnimi standardi IP68, IP69K in MIL-STD-810G. Telefon Doogee DK10 je opremljen z razmeroma zanimivo strojno opremo, še posebej za standarde robustnih telefonov. Zajema 16,9-centimetrski oziroma 6,67-palčni zaslon AMOLED ločljivosti FHD+ (1080 x 2400 slikovnih točk). Zaslon se bo dobro znašel pri praktično vsaki nalogi, tudi pri igranju iger, čeprav v osnovi temu ni namenjen. Frekvenca osveževanja namreč znaša zdaj že standardnih 120 sličic na sekundo.

Novi telefon je razumljivo najbolj primeren za delovna okolja in tiste, ki radi uživajo v naravi. V njegovi notranjosti najdemo razmeroma zmogljiv osemjedrni mobilni procesor MediaTek Dimensity 8020, 12 gigabajtov sistemskega pomnilnika in vgrajen pomnilnik s 512 gigabajti prostora za shranjevanje podatkov. Oprema obsega še baterijo kapacitete 5150 miliamper ur, ki v najboljšem primeru zadošča celo za dva ali tri dni uporabe, vsekakor pa ob koncu prvega dne še ne bo popolnoma prazna. Za njeno polnjenje je na voljo polnilec moči 120 W, kar je zelo dobrodošel dodatek. Doogee DK10 ponuja še štiri kamere, in sicer dve s senzorjema ločljivosti 50 MP, eno s 64 MP in eno s 16 MP. Za spletne konference je na voljo sprednja kamera ločljivosti 32 MP. V telefonu najdemo še podporo za dve telefonski kartici SIM ter za pomnilniško kartico kapacitete do dveh terabajtov. Nameščen je Android 13. Zanimiv Doogee DK10 lahko že kupimo v evropskem prostoru, trenutno izključno v Nemčiji. Cena pa se giblje okoli 600 evrov, kar je kar zajetna cena, ki pa so jo oboževalci očitno pripravljeni plačati.

Negativen vpliv umetne inteligence in robotov

Velika študija Inštituta za prihodnost dela iz Londona kaže, da izpostavljenost novim tehnologijam, kot so merilniki aktivnosti, roboti in umetno inteligentna programska oprema, negativno vpliva na kvaliteto človeškega življenja. V raziskavi je sodelovalo več kot 6000 ljudi, raziskovalce pa je zanimal predvsem vpliv štirih skupin tehnologij, ki postajajo vse bolj popularne.

Avtorji raziskave so ugotovili, da bolj kot so zaposleni izpostavljeni trem od teh kategorij – programski opremi, ki bazira na umetni inteligenci in tehnologiji strojnega učenja, napravam za nadzor, kot so merilniki aktivnosti in robotiki – slabše je njihovo zdravje in splošno počutje. Po drugi strani pa je uporaba dalj časa prisotnih IKT tehnologij, kot so prenosniki, tablice in komunikacijske aplikacije na delovnem mestu pokazala bolj pozitiven vpliv na počutje udeležencev raziskave. "Ugotovili smo, da se z večjo frekvenco uporabe in interakcije IKT tehnologije dviga kvaliteta življenja, medtem ko se ta niža z večjo frekvenco uporabe novejših tehnologij na delovnem mestu", so zapisali v poročilu raziskave. Avtorji sicer niso neposredno raziskovali vzrokov, so pa izpostavili, da se njihovi rezultati skladajo z ugotovitvami predhodnih raziskav, ki so pokazale, da "tovrstne nove tehnologije lahko povzročijo negotovost glede varnosti zaposlitve, povečajo obremenjenost, privedejo do rutinizacije in izgube občutka pomena opravljenega dela, prav tako pa lahko pride do izgube avtonomije in vse to vpliva na splošno počutje zaposlenih". Ekonomisti pri Goldman Sachsu ocenjujejo, da bi do leta 2030 lahko na račun avtomatizacije izginilo 300 milijonov delovnih

mest po vsem svetu. Predvsem na račun naglega razvoja generativne umetne inteligence, še veliko več vlog in delovnih mest pa se bo radikalno spremenilo, pravijo.

Dr. Magdalena Soffia, glavna avtorica raziskave pravi, da ni nujno problem sama tehnologija, temveč način, na katerega se ta uporablja. "Ne želimo trditi, da obstaja neke vrste determinizem v načinih, kako tehnologija vpliva na počutje človeka. Trdimo, da je vse odvisno od konteksta: od številnih strukturnih faktorjev, okoljskih razmer, kako je dizajnirana in kako uporabljena. Torej je tu tudi veliko človeških odločitev", pravi dr. Soffia.

Kot dodatno pojasnilo je ponudila obrazložitev, da so raziskovalci v tej študiji uporabili zelo široko sprejet model merjenja kvalitete življenja EuroQoL EQ-5D-3L. Ta zajema faktorje, kot so mobilnost, mentalno zdravje in raven bolečine. "Želeli smo zajeti bolj multidimenzionalen pogled na to, kaj se dogaja v smislu kvalitete življenja. Zato smo uporabili ta model, ki je potrjen s strani javnega zdravstvenega sektorja v Veliki Britaniji", je dodala.

Zakaj nekoliko bolj "klasična" IKT pozitivno vpliva na življenje človeka? Soffia vidi enega od potencialno možnih razlogov v tem, da pomaga olajšati delovne procese in s tem posledično dvigniti raven učinkovitosti. To pa pri ljudeh vzbudi občutek tega, da so nekaj dosegli.

Ravno nasprotno se kaže na področju uporabe

merilnikov aktivnosti in ostale tehnologije za nadzor. Sindikati na primer že nekaj časa opozarjajo na negativne vplive teh tehnologij na učinkovitost zaposlenih. Številni strokovnjaki zato kot odgovor na to študijo dodatno opozarjajo, kako pomembna je regulacija področja umetne inteligence. Kajti v nasprotnem primeru lahko pridemo do točke, kjer umetne inteligenca svet dela spremeni v nezdrav svet.

Cenejša VR očala Meta Quest 3 kmalu med nami?

Meta Quest 2 so očala za navidezno resničnost, ki jih lahko vsakdo kupi, postavi na glavo in začne uživati v navideznem svetu. So izredno enostavna za uporabo in podpirajo ogromno iger ter aplikacij. Povežemo jih lahko tudi z računalnikom, če bi na primer želeli igrati igro Half Life: Alyx. Kar dolgo so veljala za najboljši nakup, čeprav niso bila najzmogljivejša. So bila pa izredno poceni (okoli 300 evrov), zato jih je bilo težko prekositi na področju razmerja med zmogljivostjo in ceno. Še najbližje so jim prišla VR očala PICO 4. Meta Quest 2 pa so zdaj stara že 4 leta in uporabniki so zahtevali več od ponujenega. Dobili smo Meta Quest 3, nadgradnjo v vseh pogledih, na žalost tudi cenovno. Meta dvig cene upravičuje z veliko boljšo zmogljivostjo, vključno s procesorjem in kamerami za zaznavanje prostora. Cena se giblje okoli 600-700 evrov, odvisno od različice, kar je skoraj dvakrat več od osnovne različice Meta Quest 2. Meta je začutila priložnost in očitno je dovolj povpraševanja tudi za cenejšo različico najnovejših VR očal, torej Meta Quest 3 Lite.

Očala Meta Quest 3 Lite oziroma Meta Quest 3S naj bi bila opremljena s precej slabšo strojno opremo, a za to tudi z nižjo ceno. Govori se o 300 evrih ali celo manj, kar je zelo optimistična številka. Očala za navidezno resničnost Meta Quest 3 Lite naj bi bila sicer zmogljivejša v primerjavi s prejšnjim modelom Meta Quest 2, a ne bodo opremljena z naprednimi možnostmi, kot

je na primer možnost zaznave globine. Poleg tega naj bi bila izdelana iz cenejših materialov in naj bi ponujala nižjo ločljivost, 1832 x 1920 slikovnih točk namesto 2064 x 2208. Na voljo naj bi bilo tudi manj pomnilnika za shranjevanje podatkov. Vstopna različica naj bi namreč ponujala od 128 gigabajtov pa do največ 256 gigabajtov vgrajenega pomnilnika.

V primeru, da se napovedi o pametnih očalih za navidezno resničnost Meta Quest 3 Lite uresničijo, bi navidezna resničnost imela priložnost zaživeti tudi izven entuziastične skupnosti. Večje številke pa pomenijo večjo verjetnost, da se VR svetu pridružijo največji razvijalci.

Poco C61: telefon za v žep povprečnega uporabnika

Nedavna poročila so razkrila, da se bo naslednji telefon Poco serije C ob prihodu na trg imenoval Poco C61. Naprava je pred kratkim prejela odobritev certifikacijskih platform, kot sta indijski BIS in Bluetooth SIG. Prav tako je bila uvrščena v bazo podatkov platforme Google Play. Na teh seznamih je bilo navedeno, da bo telefon preoblikovana različica naprave Redmi A3, ki je pred kratkim izšla v Indiji. Glede na poročilo bo Poco C61 na voljo v dveh različicah: 4 GB RAM-a + 64 GB shrambe in 6 GB RAM-a + 128 GB shrambe. Cena pa naj bi se gibala okoli 100-150 evrov.

Poco C61 naj bi imel 6,71-palčni zaslon IPS LCD z ločljivostjo HD+ (1650 x 720 slikovnih točk), frekvenco osveževanja 90 Hz, frekvenco vzorčenja na dotik 180 Hz in največjo svetilnost 500 nitov. Zaslon bo zaščiten s steklom Gorilla Glass 3.

Poco C61 naj bi bil opremljen s čipom Helio G36, že omenjenimi 4 GB ali 6 GB pomnilnika RAM, 64 GB ali 128 GB shrambe in z režo za kartice microSD. Imel bo baterijo kapacitete 5000 mAh in podporo za 10-W polnjenje prek priključka USB-C. Imel naj bi še čitalec prstnih odtisov v gumbu za vklop in 3,5-mm priključek za slušalke, ki ga vse pogosteje najdemo samo še v telefonih nižjega razreda. Imel bo dve zadnji kameri in tudi sprednjo, vendar od zelo povprečnih senzorjev ne gre pričakovati čudežev. Lanskoletni model C51 je bil na voljo aprila, zato lahko tudi za POCO C61 pričakujemo datum izida v mesecu aprilu.

Oukitel WP36: najglasnejši telefon na trgu

Oukitelov naslednji telefon WP36 bo po zaslugi ogromne baterije s kapaciteto 10.000 mAh pričakovano namenjen za preživljanje časa na prostem brez pretiranih skrbi po polnjenju. Ker ne bo opremljen z najzmogljivejšo strojno opremo, bi morala avtonomija baterije zadoščati za večdnevno uporabo. Poleg certifikatov IP68, IP69K, MIL-STD-810H pa bo sočasno podiral še rekorde v glasnosti.

Težko je verjeti, ampak lovorika najglasnejšega telefona dejansko obstaja. In zanjo se borita dve podjetji: Oukitel in Ulefone. Ulefone je pravkar izdal prav tako izredno glasen telefon Power Armor 16S, ki ga ne bi želel videti v rokah bližnjega soseda. Oukitel je takoj vrnil udarec in predstavil model WP36.

Oukitel WP36 naj bi zmogel proizvesti zvok jakosti 128 decibelov (dB), s čimer bi presegel tudi svojega predhodnika WP22 s 125 dB. Stereo zvočni sistem 8D (do 3,5 W) bo strateško nameščen na sredini hrbtišča zadnje kamere pametnega telefona. Če malo pomižimo, lahko vidimo manjše podobnosti s telefonom Nubia Z.

Oukitelov robustni pametni telefon bo lahko služil tudi kot prenosna polnilna postaja, saj bo ogromna baterija podpirala tudi obratno polnjenje, česar ne najdemo pri telefonih Ulefone. Imel pa bo mizerno kamero ločljivosti 13 MP (Ulefone Power Armor 16S ima kamero s 50 MP). Oba pametna telefona naj bi imela 16 GB RAM-a, vendar v navezi z virtualnim RAM-om, ki črpa vire iz pogona in ni enakovreden delovnemu spominu. WP36 bo imel ob začetku prodaje večji (čeprav HD+) zaslon velikosti 6,52 palcev, poganjal ga bo procesor MediaTek MT8788, kar je njegova industrijska oznaka, zato ne vemo njegovih točnih specifikacij. Začetek prodaje bo v aprilu.

Asus ROG NUC: majhen, a močan gamer

Asus je svoj prvi računalnik ROG NUC predstavil na sejmu CES 2024. Takrat ni razkril cene, zdaj pa se šušlja, da nas bo stal okoli 2500 evrov za različico s procesorjem Intel Ultra 9 185H in grafično kartico RTX 4070. Zagotovo ne bo največji prodajni hit, morda pa bo navdušil entuziaste, ki imajo raje manjše računalnike. Sčasoma naj bi bila na voljo tudi cenejša različica s procesorjem Core Ultra 7 155H in grafiko RTX 4060. Koliko bo cenejša, ni znano, pričakuje pa se, da okoli 300-500 evrov. Ne glede na ceno je 2,5-litrski ROG NUC videti kot impresiven majhen računalnik. Specifikacije enote niso preveč zahtevne, zato hlajenje in hrup ne bi smela predstavljati težav. Vanjo lahko namestite do 64 GB pomnilnika DDR5 (SO-DIMM), tri pogone SSD PCIe Gen 4, ima pa tudi podporo za WiFi 6E, 2,5 GB LAN in Thunderbolt 4/USB 4. Slednji podpira DP 2.1, kar skupaj z dvojnim DP 1.4a in enim vhodom HDMI pomeni, da ROG NUC podpira do štiri zaslone.

ROG NUC je prvi Asusov NUC po napovedi partnerstva s podjetjem Intel. Podjetji sta se dogovorili, da bo Asus prodajal in podpiral linije izdelkov NUC od 10. do 13. generacije, hkrati pa bo Asusu zagotovil neizključno licenco za oblikovanje sistemov, kot je ROG NUC. V prihodnosti upamo na več podobnih računalnikov in morda še različice Strix in TUF.

Poceni tablica s 120-herčnim zaslonom

Tokrat imamo odlično novico za vse, ki za dobre tablične računalnike niste pripravljeni odšteti veliko. Tablični računalnik Blackview Mega 1 je na voljo v vseh večjih kitajskih spletnih prodajalnah. To pomeni, da ga lahko naročimo tudi v Slovenijo in druge države, na žalost z dodatno pristojbino. Vstopna različica novosti je trenutno na voljo za okoli 250 evrov, opremljena je z osmimi gigabajti sistemskega pomnilnika in 256 gigabajti prostora za shranjevanje podatkov.

Kot smo že poročali, je tablica Mega 1 podjetja Blackview opremljena z 11,5-palčnim oziroma 29,2-centimetrskim zaslonom z ločljivostjo 2.4K, kar je zelo presenetljiva ločljivost za tablico v tem cenovnem razredu. Sliko lahko izrisuje pri frekvenci 120 hercev, kar je super novica za gladko uporabniško izkušnjo in morebiti tudi za igranje iger. Ima ultra tanko ohišje in tehta le 528 gramov, zato bo primerna za daljša potovanja. Srce nove tablice predstavlja osemjedrni procesor MediaTek Helio G99 (jedra Cortex A76 in Cortex A55) ter soliden grafični procesor Mali G57.

Tablični računalnik Blackview Mega 1 razpolaga še z osmimi gigabajti oziroma 12 gigabajti sistemskega pomnilnika in z vgrajenim pomnilnikom kapacitete 256 gigabajtov. Slednjega lahko razširimo s pomočjo kartice microSD. Dolgo avtonomijo delovanja mu zagotavlja zmogljiva baterija kapacitete 8800 mAh. Na voljo sta še razmeroma kakovostna fotoaparata ločljivosti 50 milijonov in osem milijonov slikovnih točk in sprednja kamera ločljivosti 13 milijonov slikovnih točk. Piko na i tablici daje še lastni mobilni operacijski sistem Doke OS_P 4.0, ki temelji na osnovi sistema Android 13.

TEST

Polnilna postaja BLUETTI AC180 - ni me razočarala

Ali ste zavohali? Pomlad je tu, poletje vedno bližje. Veste, kaj to pomeni? Na žalost vrnitev komarjev in drugih nadlog, ampak tudi obdobje, ko bomo kar največ časa poskušali preživeti na prostem.

A prav na prostem nam pogosto manjka dostop do elektrike. Na test sem dobil BLUETTI prenosno polnilno postajo AC180, s katero sem želel preizkusiti, kolikšno svobodo od omrežja mi ponuja, ko nisem v bližini vtičnice. Vem, da vsakdo na to pač ne pomisli, saj ideja o preživljanju časa na prostem za mnoge pomeni sprehod, tek ali hojo v hribe in ne na primer kampiranje, potovanje z avtodomom ali piknik na odročni jasi. Za tiste, ki pa radi na tak način preživljajo svoj prosti čas, je vir energije/elektrike še kako pomemben. Postavil sem se v njihovo kožo in preizkusil, kako bi življenje na prostem izgledalo s prenosno polnilno postajo BLUETTI AC180. Postaja sicer ni njihova najnovejša, ta naziv pripada BLUETTI AC200L, a ima značilnosti, ki so zelo privlačne za povprečnega entuziasta.

Prednost	Slabosti
Visoka kapaciteta	Težje prenosljiva
Veliko različnih priključkov	Manjkajo nekateri certifikati za zunanjo rabo
Hitro polnjenje	Funkcija Power Lift bi lahko bila na voljo izven aplikacije
Priročna aplikacija	
UPS zmogljivosti	

Zajetna ne samo po kilogramih, ampak tudi po kapaciteti

Na videz skromna pravokotna škatlica skriva vrsto presenečenj. Prvo je 17 kilogramov teže, ki te preseneti, ko jo želiš prvič dvigniti. Iz tega vidika ne upraviči oznake »prenosna«, spet pa to ni teža, zaradi katere postaje nikoli ne bi uporabil na poti. Prenašanje doma med prostori in do terase bi moral preživeti vsak, ne bi je pa vzel v obzir, če bi jo moral s seboj nositi več kot 10 minut, zato vsaj zame njena raba za morebiti kakšen piknik ali zmenek na prostem odpade. Če imate avtodom, teža ne bo težava, prav tako ne za kampiranje, kadar je ta prostor seveda razumno oddaljen od avtodoma/avtomobila.

Dimenzije so ravno pravšnje za shranjevanje. Postavite jo lahko zunaj na teraso, po potrebi pod računalniško mizo, v prtljažnik – in zaradi svoje oblike ter teže se ne bo premaknila niti pri bolj agresivni vožnji skozi ovinke. Super je tudi, da bo pri naklonu terena na prostem ostala na svojem mestu in vam ne bo potrebno skrbeti, da bo na mokrem travniku zdrsnila. Za lažje prenašanje je na vsaki strani držalo, ki ne »štrli« iz ohišja, ampak se lepo zlije s celoto. To pomeni, da je vrhnja stranica popolnoma ravna, kar je dobro, če boste na primer v prtljažniku želeli izkoristiti ves prostor in na postajo postavili še kakšen drug, ne preveč težak predmet. Na vrhu je tudi postaja za brezžično polnjenje telefona, zato je ploščata stranica pravzaprav nujna, če želimo, da telefon ostane na svojem mestu. Na sredini je LCD zaslon za spremljanje porabe, kapacitete baterije in predvidene avtonomije.

Napajal sem 3D tiskalnik, laserski gravirni stroj, gaming prenosnik, telefon ...

BLUETTI AC180 ima 1152 Wh baterijo in skupno nazivno moč 1800 W, več kot dovolj za napajanje manjše elektronske naprave in tudi za nekatere bolj potratne. Med testom sem s postajo napajal več telefonov hkrati, monitor in gaming prenosnik ASUS ROG Zephyrus G16, 3D tiskalnik Creality Ender 5-S1 in potem še laserski gravirni stroj. Pričakujem, da bo najpogosteje napajala telefone in prenosnike, 3D tiskalnik in gravirni stroj pa sta dokaz, da je lahko prenosna postaja koristna tudi izven ustaljenih scenarijev. Za kratek čas sem postajo uporabil tudi na vikendu za napajanje televizorja in ročnega orodja. V aplikaciji se skriva še

funkcija Power Lift, ki omogoča napajanje bolj potratnih naprav, na primer električnega grelca, kavomata ali česa podobnega. V poštev pride tudi manjši hladilnik, ne pa na primer klimatska naprava. Aplikacija lahko deluje brez internetne povezave. Na telefonu morate imeti vklopljeno samo lokacijo in Bluetooth. V aplikaciji lahko nastavite hitrost polnjenja, vklopite AC in DC napajanje, postajo lahko tudi izklopite, vendar ponovni vklop z aplikacijo ni mogoč. Spremljate lahko porabo v realnem času in vklopite eko način za samodejni izklop po določenem času.

Na voljo sta dve 250 V (16A) vtičnici, štirje USB-A (5V) priključki, ki pa podpirajo samo napajanje z močjo 15-W, in en USB-C s podporo za 100-W polnjenje, kar je zagotovo dobrodošlo, bi si pa morda želel kakšen USB-C več. Kot rečeno, na vrhu je 15-W brezžični polnilnik, kar je prav tako lahko priročno, če imate telefon, ki podpira brezžično polnjenje. To so praktično vsi premijski modeli in tudi kakšen iz višjega srednjega razreda.

Na voljo je še 12V (10A) vtič, kot ga najdemo v avtomobilu. Prenosno polnilno postajo lahko preko navadne vtičnice napolnimo v približno eni uri. Polni se z močjo 1440 W, po želji pa si lahko dokupite tudi solarni komplet, s katerim boste postajo polnili z močjo 500 W, seveda odvisno od zunanjih razmer. Ljubitelji avtodomov in entuziasti, ki ste svoje avtomobile in kombije spremenili v potujoči hotel, pa lahko prav tako izkoristite polnjenje preko avtomobilskega priključka. Ne bo ravno hitro, a si boste med potovanjem povrnili vsaj kakšen odstotek baterije.

BLUETTI AC180 uporablja LiFePo4 baterije, ki za katodo uporabljajo železov fosfat. Njihova prednost je boljša stabilnost, varnost in tudi veliko daljša življenjska doba v primerjavi s klasičnimi NCM in NCA baterijami. BLUETTI pravi, da bo baterija dosegla 3500 polnilnih ciklov, preden bo kapaciteta padla na 80 %, kar AC180 uvršča med najboljše na trgu. Med 3D tiskanjem sem v slabi uri porabil 15 %, malenkost več energije mi je ostalo pri laserskem gravirnem stroju. Pri uporabi prenosnika bi mi polno napolnjena postaja zadoščala za 8-urni delavnik, pri igranju iger pa se je računica ustavila nekje pri 4 urah. Eno popoldne je BLUETTI AC180 preživel tudi z napajanjem manjšega televizorja, grelnika vode in manjših orodij (mešalnik, brusilk) za delo na vikendu.

Ali je postaja glasna? Ni tiha, ni pa tudi pretirano glasna. Še najbolj se jo sliši med Turbo polnjenjem ali pa pri res visoki porabi.

Za trenutek sem jo uporabil tudi kot UPS. Namerno sem povzročil izpad energije in opazoval, kako hitro preklopi napajanje. Testni zajček je bil moj stari prenosnik brez delujoče baterije in očitno je bil zakasnitveni čas tako nizek, da je prenosnik ostal priklopljen.

Ali sem sploh našel kakšno slabost?

Ne veliko. Najbolj me je ovirala teža. Zaradi priročnih ročajev sem jo lahko nosil z eno roko, ampak ne predstavljam si, da bi obenem nosil še druge stvari, ki bi jih morebiti potreboval za kampiranje ali drugo dejavnost na prostem. Vzemite v roke 20-kilogramsko utež, začnite hoditi in si zapomnite, koliko časa ste hodili brez težav.

Funkcija Power Lift bi lahko bila na voljo tudi izven aplikacije, ni pa to nujna sprememba. Moj zadnji pomislek je, da polnilna postaja uradno nima certifikatov za varno uporabo na prostem. Govorim o zaščiti pred tujki, vodo in ostalimi delci, ki bi lahko vplivali na njeno delovanje. Če jo boste uporabljali na prostem, ni nič narobe, če ji najdete prostor, kjer bo ostala suha in na varni razdalji od neposredne umazanije.

Če potrebujete napajanje izven doma …

… je BLUETTI AC180 zelo dobra polnilna postaja, ki me ni razočarala. Napaja lahko skoraj vse najbolj uporabljene naprave, nekatere tudi istočasno. Priključkov je dovolj, kakovost izdelave je odlična. Teža je lahko pri določenih primerih uporabe ovira, vendar boste težko našli polnilno postajo z enako kapaciteto in občutno manjšo težo.

Več na www.bluettipower.com.

Kibernetska varnost je ključavnica, ključ je v vaših rokah

Kibernetska varnost je ključna komponenta digitalne dobe, zagotavlja zaščito podatkov, omrežij in sistemov pred digitalnimi napadi.

S hitrim napredkom tehnologije se povečujejo tudi kibernetske grožnje, kar zahteva stalno prilagajanje in razvoj varnostnih strategij. Kibernetska varnost je multidisciplinarno področje, ki zahteva poglobljeno razumevanje različnih elementov in tega, kako ti medsebojno delujejo za zagotavljanje celovite zaščite digitalnih sredstev.

Zaupnost, integriteta in razpoložljivost

Temeljni koncept v kibernetski varnosti, ki oblikuje osnovo za razvoj in implementacijo varnostnih politik ter praks, predstavljajo zaupnost (angl. confidentiality), integriteta (angl. integrity) in razpoložljivost (angl. availability), vsak element pa igra ključno vlogo pri zagotavljanju celovite varnosti informacijskih sistemov in podatkov.

Zaupnost se osredotoča na preprečevanje nepooblaščenega dostopa do občutljivih informacij. Cilj je zagotoviti, da podatki ostanejo skriti tistim, ki za dostop niso pooblaščeni. Tako je varovana zasebnost posameznikov in varnost organizacij. Šifriranje je glavno orodje za ohranjanje zaupnosti. Šifriranje pretvori občutljive podatke v nečitljivo obliko, ki jo lahko dešifrirajo samo tisti z ustreznim ključem. Nadzor dostopa je enako pomemben element pri zagotavljanju zaupnosti. S sistemi za nadzor dostopa se lahko dodeljuje pravice in omeji uporabnikom dostop do informacij ali virov na osnovi njihove vloge, odgovornosti ali potrebe po dostopu. Uporaba gesel, biometričnih podatkov in drugih metod preverjanja identitete zagotavlja, da samo pooblaščeni uporabniki dostopajo do zaščitenih virov.

Integriteta zagotavlja, da so informacije pristne, natančne in nedotaknjene skozi celoten življenjski cikel. Zaščita integritete preprečuje nepooblaščene spremembe podatkov, bodisi zaradi napadov, napak v programski opremi ali človeških napak. Kriptografski »hashi« se uporabljajo za preverjanje neokrnjenosti podatkov. Vsaka sprememba podatkov se bo pokazala v drugačnem hashu, s čimer se odkrijejo manipulacije. Digitalni podpisi omogočajo preverjanje izvora in integritete podatkov, saj zagotavljajo, da je bilo sporočilo, ki ga je podpisala določena oseba, prejeto v originalni, nespremenjeni obliki.

Razpoložljivost se nanaša na zagotavljanje, da so informacije in sistemi dostopni pooblaščenim uporabnikom, ko jih potrebujejo. To vključuje zaščito pred napadi, ki ciljajo na motnje delovanja ali dostopnosti, kot so DDoS napadi. Pri tem je izredno pomembna redundanca podatkov. S kopiranjem podatkov na več lokacij ali medijev zagotavlja, da so informacije dostopne tudi v primeru okvare strojne opreme, naravnih katastrof in podobno. Potrebno je misliti tudi na obremenitev in pravilno distribucijo prometa med več strežniki, s čimer si zagotovimo neprekinjeno dostopnost storitev.

Pravilno uravnoteženje teh treh elementov omogoča organizacijam, da svoje vire zaščitijo na način, ki podpira njihove poslovne cilje in zahteve, hkrati pa zmanjšuje tveganje za izgubo podatkov, kršitve varnosti in druge potencialne varnostne incidente.

Vsaka od treh komponent (zaupnost, integriteta in razpoložljivost) zahteva specifične strategije in tehnologije za njeno učinkovito izvajanje. Napredovanje v tehnologiji prinaša nove izzive in

grožnje, kar zahteva stalno ocenjevanje in prilagajanje varnostnih ukrepov. Varnostne ekipe morajo biti proaktivne pri odkrivanju novih ranljivosti, pri čemer se zanašajo na stalno izobraževanje, raziskave in uporabo naprednih orodij za zaščito pred nenehno spreminjajočo se pokrajino groženj.

Kaj varuje omrežja?

Omrežna varnost je še ena pomembna sestavina kibernetske varnosti, ki se osredotoča na zaščito infrastrukture in podatkov, ki se prenašajo in upravljajo preko računalniških omrežij. Z vse večjim številom napadov, usmerjenih na omrežne vire, postaja implementacija robustnih omrežnih varnostnih ukrepov nujna. Požarni zidovi delujejo kot pregrada med zaupanja vrednim notranjim omrežjem in nezaupanja vrednimi zunanji omrežji, kot je internet. Filtrirajo dohodni in odhodni promet na osnovi določenih pravil in politik, preprečujejo nepooblaščen dostop in napade.

Sistemi za preprečevanje vdorov (IPS) in za odkrivanje vdorov (IDS) nadzorujejo omrežni promet in skenirajo morebitne sumljive dejavnosti, ki bi lahko nakazovale na napad ali vdor. IDS sistemi opozarjajo administratorje o potencialnih grožnjah, medtem ko IPS sistemi dejansko blokirajo promet, ki je identificiran kot škodljiv.

Virtualna zasebna omrežja (VPN) omogočajo varno povezavo med oddaljenimi uporabniki in omrežjem podjetja preko šifrirane komunikacijske poti. To je še posebej pomembno za oddaljeno delo, saj tehnologija zagotavlja, da so podatki, ki se prenašajo preko nezavarovanih omrežij, kot je internet, zaščiteni.

Določena varnostna tveganja se povečujejo tudi z naraščajočo uporabo brezžičnih omrežij. Ukrepi za brezžično varnost vključujejo šifriranje WPA/WPA2/WPA3, skrivanje SSID, filtriranje MAC naslovov in segmentacijo gostujočih omrežij. Segmentacija omrežja deli omrežje na manjše, lažje upravljive segmente, ki jih je mogoče individualno varovati. To ne samo omejuje obseg potencialnega napada, ampak tudi olajša nadzor nad prometom in dostopom.

Napredni sistemski monitorji in orodja za analizo omrežja omogočajo spremljanje omrežnega prometa v realnem času, identifikacijo nenavadnih vzorcev ali anomalij, ki bi lahko nakazovale na varnostne incidente. Človeški faktor pogosto predstavlja najšibkejšo točko v omrežni varnosti. Ključnega pomena je redno usposabljanje zaposlenih o varnostnih grožnjah, kot so phishing napadi, in najboljših praksah za varno uporabo omrežnih virov. Razvoj jasne varnostne politike, ki določa pričakovanja, pra-

vila in postopke za upravljanje in zaščito omrežnih virov, je temelj učinkovite omrežne varnosti. Enako pomembni so tudi dobro opredeljeni postopki odziva na incidente, ki zagotavljajo hitro in učinkovito ukrepanje.

Kaj je aplikacijska varnost in kaj vse zajema?

Aplikacijska varnost se nanaša na ukrepe in procese, ki se uporabljajo za preprečevanje ranljivosti v aplikacijah, bodisi v fazi razvoja bodisi ko so aplikacije že v uporabi. Z vzponom spletnih storitev in mobilnih aplikacij postaja aplikacijska varnost ključni element v širšem spektru kibernetske varnosti, saj napadalci pri napadih vedno bolj ciljajo na aplikacijsko plast.

Zato je pomembno varnostno kodiranje, ki je proces vključevanja varnostnih praks neposredno v razvoj aplikacij in vključuje omejevanje dostopa in funkcionalnosti na najmanjšo možno mero, ki je potrebna za delovanje aplikacije, preverjanje vhodnih podatkov za preprečevanje injekcijskih napadov, kot sta SQL injection ali XSS. Šifriranje tudi tukaj ponovno igra močno vlogo za zaščito občutljivih podatkov, bodisi tistih shranjenih v aplikaciji bodisi informacij v prenosu.

Avtomatizacija varnostnih pregledov in testov lahko pomaga zgodaj odkriti ranljivosti v razvojnem ciklu, kar zmanjšuje stroške popravil in povečuje varnost aplikacij. Integracija varnostnih orodij v CI/CD cevovode (angl. pipeline) je prva stopnička do avtomatizacije varnostnih pregledov. Redno skeniranje lahko odkrije zastarele knjižnice in okvirje, ki vsebujejo znane ranljivosti.

Z vključevanjem varnostnih praks v vsak korak razvojnega cikla, od začetne zasnove do izdaje in vzdrževanja, organizacije ne samo zmanjšujejo tveganje za varnostne incidente, ampak tudi krepijo zaupanje uporabnikov v svoje izdelke.

Katere so najbolj pereče kibernetske grožnje?

Med najpogostejše kibernetske grožnje sodijo ransomware napadi. Ransomware je oblika zlonamerne programske opreme, ki šifrira datoteke na napadenem sistemu, žrtvi pa onemogoča dostop do lastnih podatkov brez ključa za dešifriranje, ki ga napadalec običajno ponudi v zameno za plačilo odkupnine. Izvedba napada z ransomware se običajno začne z uspešno izvedenim vdorom v sistem, kar napadalci dosežejo na več načinov.

Najprej je lahko tarča okužena preko zlonamernih prilog ali povezav v phishing elektronskih sporočilih, ki se zdijo legitimna. Ko uporabnik odpre prilogo ali klikne na povezavo, se izvrši zlonamerni skript, ki začne postopek šifriranja podatkov. Druga metoda vključuje izkoriščanje ranljivosti v programski opremi, ki je nameščena

na sistemu tarče napada. To pomeni, da napadalci iščejo sisteme, ki niso bili posodobljeni ali popravljeni za znane varnostne luknje, skozi katere lahko nepopaženo vstavijo ransomware.

Phishing napadi predstavljajo eno od najpogostejših in najučinkovitejših metod kibernetskih napadov in temeljijo na socialnem inženiringu. Cilj teh napadov je pridobiti občutljive informacije, kot so gesla, podatki o bančnih računih ali druge osebne informacije, tako da napadalci manipulirajo z žrtvami, ki jim te informacije prostovoljno predajo. Phishing napadi se običajno izvajajo preko elektronskih sporočil, ki se zdijo, da prihajajo iz zaupanja vrednih virov, kot so banke, socialna omrežja, ponudniki spletnih storitev ali celo sodelavci znotraj iste organizacije.

Napadalci skrbno oblikujejo ta sporočila, da so videti legitimno, pogosto z uporabo uradnih logotipov, podpisov in sloga komunikacije, ki posnema pravi vir. Sporočila lahko vsebujejo prepričljive pozive k ukrepanju, kot so trditve o sumljivih dejavnostih na računu žrtve, nujnih posodobitvah sistema ali potrebah po preverjanju identitete. Povezave znotraj teh sporočil vodijo do ponarejenih spletnih strani, ki so prav tako skrbno oblikovane, da izgledajo kot pristne spletne strani ciljanih institucij.

Kaj pa so »zero-day« ranljivosti oziroma ranljivosti ničelnega dne? Te predstavljajo vrzel v varnosti programske opreme, ki je še neodkrita s strani razvijalcev ali proizvajalcev te programske opreme. Ime "zero-day" izhaja iz dejstva, da nimajo razvijalci "nič dni časa" za odpravo te ranljivosti, saj je že bila izkoriščena ali pa obstaja možnost, da bo s strani napadalcev izkoriščena, preden bo javno znana. Te ranljivosti predstavljajo posebno nevarnost, ker zanje običajno ni na voljo popravka ali zaščite, kar napadalcem omogoča, da brez zaznavanja prodirajo v sisteme in izvajajo svoje napade.

Napadalci izkoriščajo ranljivosti ničelnega dne za različne namene, vključno z distribucijo zlonamerne programske opreme, krajo občutljivih podatkov, pridobivanje nepooblaščenega dostopa do sistemov ali izvajanje drugih škodljivih aktivnosti. Zaradi narave teh ranljivosti so napadi običajno zelo sofisticirani in ciljajo na specifične, visoko vredne tarče, kot so vladne agencije, velike korporacije ali infrastrukturni sistemi.

Posebej zahrbtne so tudi grožnje iz notranjosti organizacij (t.i. insider threats), saj izvirajo od posameznikov z legitimnim dostopom do sistemov in podatkov, ki lahko iz malomarnosti ali zlih namenov povzročijo škodo.

Novo fronto kibernetskih groženj pa predstavljajo varnostne ranljivosti IoT (internet stvari) naprav. Povečano število povezanih naprav v gospodinjstvih in industriji ustvarja več vstopnih točk za napadalce. Ti napadi lahko segajo od vdorov v zasebnost do množičnih DDoS (napad za zavrnitev storitve) napadov, ki izkoriščajo nezavarovane IoT naprave za preplavljanje ciljnih omrežij s prometom.

Ker danes praktično ni naprave, ki ne bi bila povezana na omrežje, se bo pomen kibernetske varnosti le še povečeval. S prihodom umetne inteligence smo dobili novo močno orodje za obrambo, a istočasno so tudi napadalci dobili močno orožje za izvajanje kompleksnejših napadov. Ujeti smo v cikel, ki mu ni videti konca.

HIKVISION

Inovativne tehnologije za izboljšanje varnosti vašega doma

Lastniki domov in ostalih nepremičnin želijo biti prepričani, da je njihova lastnina varna, tudi ko jih ni v bližini. Hikvisionovi tehnologiji AX PRO in ColorVu zagotavljata večdimenzionalno varnost in oddaljeno preverjanje varnostnih incidentov, s čimer rešujeta tehnične izzive tradicionalnih rešitev.

Tradicionalni alarmni sistemi lahko obvestijo lastnike domov in podjetij, da obstaja morebitna težava, ne pa točno, kaj se dogaja. Za zagotavljanje izboljšane varnosti in popolne brezskrbnosti Hikvisionov brezžični alarmni sistem AX PRO zagotavlja alarme z video izsekom, kar omogoča preverjanje varnostnih incidentov in zagotavlja slikovne ali video dokaze v realnem času – neposredno na mobilni telefon uporabnika.

Poleg tega Hikvisionova tehnologija ColorVu zagotavlja barvno sliko, tudi do 0,0005 luksa, kar je enako svetlobi, ki jo zagotavljajo zvezde ponoči. Barvne slike zagotavljajo veliko več podrobnosti, kar olajša identifikacijo storilca in poveča kakovost dokazov za kasnejšo uporabo.

Brezžični alarmni sistem AX PRO ima za lastnike domov in podjetij tri glavne prednosti

1) "Alarmi z video preverjanjem" za izboljšano varnost

Tradicionalni varnostni alarmni sistemi omogočajo obveščanje, da obstaja težava, vendar so podrobnosti včasih nejasne, pogosti pa so tudi lažni alarmi. Sistem AX PRO se bori proti temu z "video preverjanjem", kar pomeni, da si lahko lastniki ogledajo videoposnetke ali dostopajo do GIF slik na daljavo prek aplikacije HikConnect na svoji mobilni napravi. Poleg tega detektor AX PRO PIRCAM v primeru vloma pošlje do 20 fotografij, kar omogoča takojšen pregled incidenta, ter hiter in učinkovit odziv.

Z aplikacijo HikConnect je mogoče fotografije in video dokaze incidentov v realnem času poslati tudi v centre za sprejem alarmov (ARC), kar varnostnim ekipam omogoča vpogled v realnem času in jim je v pomoč pri hitrem in ustreznem odzivu.

2) Večdimenzionalna varnost za popolno brezskrbnost

Širok izbor razpoložljivih naprav AX PRO zagotavlja maksimalno varnostno zaščito domov in poslovnih prostorov. Z visoko zanesljivimi magnetnimi detektorji, detektorji razbitja stekla in »varnostnimi zavesami« je vsak vlom takoj zaznan. Še več, namenski detektorji AX PRO lastnike domov in podjetij zgodaj opozorijo na puščanje vode, dim in temperaturne spremembe, kar jim omogoča, da se hitro odzovejo, preden pride do kakršne koli škode.

3) Manj lažnih alarmov in manj skrbi

Alarmne naprave AX PRO, ki jih poganjajo vgrajeni algoritmi globokega učenja, lahko razlikujejo med hišnimi ljubljenčki in drugimi nedolžnimi premikajočimi se predmeti ter resničnimi varnostnimi grožnjami. To pomeni, da lastniki stanovanj porabijo manj časa in energije za preiskovanje lažnih alarmov, ter zmanjšajo stres. Druga prednost je zmožnost osredotočanja časa in virov samo na resnične varnostne grožnje in zmanjšanje stroškov delovanja nadzornega centra na podlagi lažnih alarmov.

Odklenite neomejene možnosti s tehnologijo ColorVu

Dobra vidljivost je pri videonadzoru ključnega pomena, zlasti v zahtevnih svetlobnih pogojih, ko je svetloba prešibka. S Hikvisionovo revolucionarno tehnologijo ColorVu postavljajo tehnologijo snemanja pri šibki svetlobi na povsem novo raven. Predstavljajte si na primer scenarij, ko poskuša vsiljivec v temi vdreti v varovani objekt. Neprimerljive zmogljivosti ColorVu zagotavljajo žive in podrobne slike vlomilca, ki strokovnjakom za varnost omogočajo, da prepoznajo grožnjo in se hitro odzovejo, kar zagotavlja varnost in brezskrbnost za vse.

1) Nastavljiva jasnost z »varifokalnimi« kamerami

»Varifokalne« kamere, ki podpirajo ColorVu tehnologijo, se s prilagajanjem goriščne razdalje dinamično prilagodijo različnim scenarijem. Z veliko fiksno zaslonko F1.0 te kamere med približevanjem (zoom) ohranjajo konstantno svetlost slike in zagotavljajo neprimerljivo vidljivost.

2) Inteligentna integracija

S kombinacijo tehnologije ColorVu in AcuSense kamere Hikvision natančno zaznavajo in razlikujejo med ljudmi in vozili. Ta integracija izboljša podrobnosti predvajanja videa in poenostavi iskanje posnetkov, kar zagotavlja pametnejšo zaščito. Tehnologijo AcuSense poganja Motion Detection 2.0, ki razlikuje med ljudmi/vozili in drugimi predmeti ter se osredotoča na resnične varnostne grožnje.

Hikvisionova rešitev AX PRO in tehnologija ColorVu skupaj z drugimi naprednimi rešitvami Hikvision razširjata možnosti za reševanje varnostnih problemov v različnih situacijah, seveda tudi pri varovanju doma. Za več podrobnosti obiščite spletno stran www.hikvision.com/europe. (P.R.)

HIKVISION
adriatic-malta@hikvision.com
www.hikvision.com/europe

LENOVO

Moč in prilagodljivost podatkovnih sistemov Lenovo

Dostopnost podatkov postaja osrednji vir konkurenčne prednosti, podjetja pa iščejo napredne podatkovne rešitve, ki lahko zadovoljijo njihove vedno večje in zahtevnejše potrebe.

Lenovo, kot vodilno podjetje na tem področju, ponuja raznolike rešitve za shranjevanje podatkov, ki so prilagojene sodobnim izzivom, hkrati pa so cenovno dostopne in zanesljive. Na trgu izstopajo modeli iz serij ThinkSystem DM in DE, v praksi pa naprave prinašajo številne koristi.

Lenovo podatkovni sistemi

Lenovo nudi širok razpon rešitev za shranjevanje podatkov v podjetjih, ki so oblikovane tako, da ustrezajo proračunom in zahtevam posameznega podjetja in zagotavljajo, da so podatki dostopni vedno, ko jih potrebujete. Te rešitve vključujejo ključne funkcionalnosti za učinkovitost podatkov, kot so stiskanje in zgoščevanje, thin-provisioning ter šifriranje podatkov z uporabniku prijaznim vmesnikom. Dodatne varnostne funkcije, kot so šifriranje na sami napravi, večfaktorsko preverjanje pristnosti in sinhrono kopiranje, predstavljajo le nekaj izmed vodilnih funkcionalnosti upravljanja podatkov, ki jih Lenovo nudi svojim uporabnikom.

Predstavitev modelov: ThinkSystem DM in DE

ThinkSystem DM (osnovna serija)

DM serija podpira flash in hibridne-flash diske, ki so pripravljeni na oblak, virtualizacijo in umetno inteligenco. Te naprave omogočajo optimizacijo, pospeševanje in združevanje podatkov z združevanjem SAN in NAS v enem sistemu. Modeli, kot so DM7100H, DM5000H, DM3010H in DM3000H, so namenjeni za delo z oblačnimi storitvami, umetno inteligenco, analitiko velikih podatkov in za oblikovanje.

ThinkSystem DE (naprednejša serija)

DE serija vključuje flash in hibridne-flash diske, ki zagotavljajo idealno kombinacijo zmogljivosti in učinkovitosti za zagotavljanje najzahtevnejših potreb. Modeli, kot so DE6400H, DE6600H in DE6000H, so popolni za širok spekter podjetniških delovnih obremenitev, vključno z analitiko velikih podatkov, videonadzorom, varnostnim kopiranjem in obnavljanjem ter drugimi aplikacijami z intenzivnim vhodno/izhodnim delovanjem.

Reševanje ključnih izzivov

Lenovo podatkovne rešitve so osredotočene na reševanje štirih ključnih izzivov, s katerimi se podjetja soočajo danes: virtualizacija, prilagodljivost, hibridne in oblačne storitve ter razširljivost. S sposobnostjo prilagajanja potrebam poslovnega okolja, Lenovo rešitve omogočajo podjetjem, da svoje podatkovne centre prilagodijo in optimizirajo brez kompromisov pri zmogljivosti ali varnosti.

Zakaj izbrati Lenovo?

Cenovna ugodnost

Analiza cenovne učinkovitosti je že leta 2018 pokazala, da Lenovo nudi visoko zmogljive podatkovne rešitve po dostopnih cenah, kar omogoča podjetjem, da izkoristijo napredno tehnologijo brez prekomernih stroškov.

Zanesljivost

Po najnovejših podatkih iz marca 2024, Lenovo strežniki ostajajo na vrhu tudi po zanesljivosti, kar se odraža tudi v Lenovo podatkovnih rešitvah, ki sledijo isti viziji stabilnosti in dolgotrajne zanesljivosti.

Hitrost

Kar zadeva hitrost, Lenovo shrambne rešitve zagotavljajo vrhunsko delovanje, ki presega konkurenco. ThinkSystem DM in DE serije s flash in hibridnimi-flash konfiguracijami podjetjem omogočajo hitro dostopanje do kritičnih podatkov, hkrati pa ohranjajo visoko stopnjo učinkovitosti in odzivnosti.

Zakaj ukrepati zdaj?

Podjetja morajo danes nujno sprejeti rešitve, ki ne samo zadovoljujejo trenutne potrebe, ampak so pripravljene tudi na prihodnje izzive. Lenovo s svojimi podatkovnimi rešitvami ponuja prav to: tehnologijo, ki je pripravljena na prihodnost, je cenovno dostopna in zanesljiva. Ne zamudite priložnosti, da izboljšate svoje podatkovno shranjevanje in poslovanje z naprednimi Lenovo rešitvami. Več najdete na spletni strani https://bit.ly/also-lenovo. (P.R.)

ALSO Technology Ljubljana, d.o.o.

Ukmarjeva ulica 2, 1000 Ljubljana
info.si@also.com
+386 1 4205 506

DAHUA TECHNOLOGY SLOVENIJA

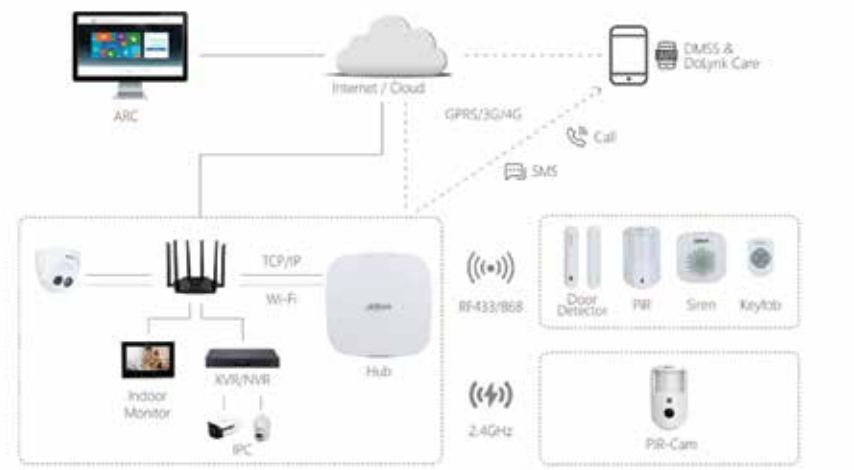
Dahua AirShield - neprebojen oklep okoli vašega doma

Varnost je vznemirljiva tema. Ko že misliš, da si spoznal najboljšo rešitev za zavarovanje svojega doma ali podjetja, naletiš na nov koncept, ki te v celoti prevzame in razmišljaš samo še, kako bi ga lahko uporabil za svoje potrebe.

Začne se s kamerami, ki jih postavimo v vsak kotiček zunaj in znotraj našega doma ali podjetja. Kasneje dodamo senzorje gibanja, detektorje dima, plina in podobno, končamo pa z alarmnimi vozlišči. Potem pa ugotovimo obstoj še boljšega sistema Dahua AirShield, ki lahko naše posamezne varnostne naprave zedini v eno celoto in ustvari brezžični oklep okoli doma.

Dahua AirShield vas varuje brezžično

Dahua AirShield se zanaša na tehnologije Airfly 3.0, RF-HD in na oblak za zanesljivo in varno komunikacijo med različnimi komponentami vašega varnostnega sistema, vključno z alarmi, kamerami, pametnimi vtičnicami, različnimi senzorji, detektorji, repetitorji in podobnimi napravami. Podpira povezovanje z do 150 brezžičnimi napravami, kar je več kot dovolj za varovanje povprečnega doma in zadosti tudi za manjše poslovne objekte.



Sistem AirShield je skladen s standardi EN50131 Grade-2, kar zagotavlja visoko raven varnosti in zanesljivosti. Tehnologija Airfly 3.0 za povezovanje s perifernimi napravami uporablja kanala 433 in 868 MHz. Tehnologija Airfly je znana po zanesljivosti, dolgem dosegu in stabilnosti. Komunikacijo varuje šifriranje AES128 in še dodatne funkcije, kot je skakanje frekvenc, ki preprečuje motnje signala med vozliščem in povezanimi napravami.

RF-HD uporablja 2,4-GHz spekter za hitrejši slikovni prenos pri visoki ločljivosti, kar je odlično za prenos slike iz nadzornih kamer v realnem času, kar vam omogoča takojšen odziv na incident ali pa morebitno hrambo visokoločljivostnega posnetka kot dokaznega materiala.

Na voljo je še povezovanje z oblakom, ki sistemu omogoča sprejemanje obvestil v realnem času in upravljanje na daljavo prek mobilne aplikacije, kar uporabnikom in inštalaterjem zagotavlja prilagodljivost pri nadzoru alarmnih sistemov ne glede na njihovo lokacijo.

Z uporabo oblaka AirShield sistem izboljša zanesljivost in razširljivost, omogoča lažje posodobitve programske opreme in vzdrževanje sistema ter omogoča učinkovito dvosmerno komunikacijo med centralnim vozliščem in povezanimi brezžičnimi napravami. To vključuje sposobnost sistema, da se poveže z različnimi omrežnimi načini, kot so Ethernet, Wi-Fi, GPRS, 3G in 4G (odvisno od vozlišča), kar zagotavlja neprekinjeno komunikacijo z oblakom ali spremnikom ARC – ne glede na lokalne omrežne pogoje. AirShield sistem brez težav sodeluje tudi z Dahua NVR/XVR ali Android videodomofoni (VTH), kar povečuje funkcionalnost ob znižanju stroškov z več povezovalnimi možnostmi. Preko naprave VTH lahko uporabnik vklopi ali izklopi celotni varnostni sistem, enostavno pregleda stanje povezanih naprav, ustvari profile in jim dodeli ustrezna dovoljenja za upravljanje z alarmnim sistemom.

Neomajna varnost, ki jo potrebuje vsak dom

Dahua AirShield je odlična rešitev za varnost domov in podjetij. Namestitev je enostavna, komunikacija brezžična in varna, uporabnik pa se lahko zanaša na visoko zanesljivost, prijazno uporabniško izkušnjo in oddaljeno upravljanje, s katerim si lahko v realnem času ogledamo vsak trenutek, ki se je zgodil pod budnim očesom varnostnega sistema Dahua AirShield.

Če bi radi izboljšali varnost svojega doma ali podjetja, obiščite www.dahuasecurity.com. (P.R.)

Dahua Technology Slovenija
Cesta na Okroglo 7, 4202 Naklo
www.dahuasecurity.com

NEOSERV: SPLETNO GOSTOVANJE IN DOMENE

WordPress: kako poskrbeti za varnost spletne strani?

WordPress je daleč najpogosteje uporabljena platforma za postavitev spletne strani, s tem pa tudi pogosta tarča spletnih virusov in napadalcev. Če tudi vaše spletno mesto temelji na sistemu WordPress, ne spreglejte nasvetov, kako temeljito poskrbeti za njegovo varnost.

Pri NEOSERV, enem največjih ponudnikov spletnega gostovanja v Sloveniji, opažajo, da ima velika večina njihovih naročnikov svoja spletišča postavljena v sistemu WordPress. Tudi podatki W3Techs kažejo na visoko priljubljenost omenjene platforme, saj naj bi skoraj vsako drugo spletno mesto temeljilo na **WordPressu**. Njegova izjemna popularnost pa je hkrati razlog, da je sistem **pogosta tarča vdorov, zlonamernih kod in virusov**, ki lastnikom spletnih mest povzročajo škodo. Še posebej, ko gre za spletne trgovine, je ta lahko izjemno velika. Ali tudi vaše spletno mesto temelji na omenjenem sistemu? Potem je vsekakor nujno, da spoznate bistvene ukrepe za **povečanje varnosti vašega WordPress spletišča** in jih v čim krajšem času realizirate. Nikoli namreč ne veste, kdaj bo zlonamerna skripta "obiskala" vašo spletno stran. Morda ravno jutri.

Varno geslo in dvostopenjska avtentikacija

Osnovni korak k varnosti je uporaba močnega gesla, ki ga uporabljate za prijavo v WordPress administracijo. Geslo naj sestoji iz vsaj 12 znakov, sestavljeno pa naj bo iz malih in velikih črk, številk in posebnih znakov. Poskrbite tudi za dvostopenjsko avtentikacijo (2FA), ki jo dosežete z namenskim vtičnikom (npr. miniOrange Google Authenticator).

Originalne grafične predloge in vtičniki

Vedno se poslužujte le originalnih WordPress grafičnih predlog in vtičnikov. Številne brezplačne vtičnike in grafične predloge boste našli na spletnem naslovu WordPress.org, kjer velja preveriti datum zadnje posodobitve. Vtičnikov in predlog, ki jih razvijalci že dolgo niso posodobili, ne uporabljajte. Plačljive predloge in vtičnike iščite na preverjenih platformah, kot sta ThemeForest in CodeCanyon.

Redno posodabljanje vseh komponent

Korak za varnost, pri katerem največ lastnikov WordPress spletišč naredi napako, je redno posodabljanje spletne strani. Izjemno pomembno je, da posodobitve opravljate dosledno in sistematično, pri čemer ne smete pozabiti na nobeno izmed treh komponent, ki sestavljajo vaše WordPress spletno mesto: jedro (ang. core), vtičniki (ang. plugins), grafična predloga (ang. template).

Uporaba varnostnega vtičnika

Svetujemo uporabo vtičnika Wordfence Security, ki je na voljo tako v plačljivi kot brezplačni različici. Že brezplačna verzija prinaša učinkovite funkcionalnosti, kot so pregled datotek WordPress jedra, vtičnikov in grafične predloge, odstranjevanje morebitne zlonamerne kode, blokiranje IP naslovov ali držav, zaščita spletišča s požarnim zidom, onemogočanje zaporednih poskusov vpisa v administracijo, aktivacija dvostopenjske avtentikacije, obveščanje o poskusih vdora na e-naslov in še mnogo več.

Varno spletno gostovanje

Varnost je, poleg zanesljivosti in hitrosti, izjemno pomemben element spletnega gostovanja, saj vpliva na stabilnost in delovanje spletnih storitev, zaščito podatkov ter zasebnost uporabnikov. Pri **NEOSERV** se tega dobro zavedajo, zato so tako v WordPress gostovanje kot v vse druge vrste spletnega gostovanja implementirali **napredno tehnologijo antivirusne zaščite**, ki samodejno zazna morebitne varnostne luknje v spletnih straneh in jih zakrpa. Obenem zaščita samodejno očisti tudi obstoječe viruse, npr. po prenosu spletne strani od drugega ponudnika gostovanja na njihov strežnik, če se izkaže, da je spletišče že pred prenosom vsebovalo zlonamerno kodo. Postopek iskanja in saniranja virusov je za lastnika splene strani in obiskovalce neopazen, saj se procesi izvajajo v ozadju in ne vplivajo na delovanje strani.

Ekipa NEOSERV svojim naročnikom spletnega gostovanja zagotavlja **celovit pristop k varnosti,** s katerim skrbi za visok nivo zaščite in zanesljivosti storitve. Ponudnik zagotavlja tudi brezplačne varnostne kopije vseh podatkov (spletne strani, e-poštni predali) na dnevni, tedenski in mesečni ravni. Prav tako pa velik poudarek daje **hitrosti delovanja spletnih strani**, kar primarno dosega z investicijami v najsodobnejše strežnike proizvajalca Dell ter z uporabo naprednih NVMe SSD diskovnih enot in bliskovito hitre tehnologije LiteSpeed.

Več informacij lahko najdete na spletni strani www.neoserv.si. (P.R.)

IT-OPTI

Varno in učinkovito IT upravljanje

Podjetja se pri poslovanju vedno bolj zanašajo na tehnologijo, pri tem pa lahko težavo predstavlja vzdrževanje računalniške opreme in varnost. Za to poskrbi IT-OPTI.

Če si želi podjetje zagotoviti digitalno prihodnost, mora za to poskrbeti že danes. Pogosto je najboljša rešitev sodelovanje s ponudnikom, ki lahko poskrbi za široko paleto rešitev na enem mestu.

To pogosto vključuje prodajo, vzdrževanje in servis računalniške opreme, najem strežnikov, varnostne kopije, nadzor, svetovanje …

Vzdrževanje in servis računalniške opreme

IT-OPTI je specializiran za vzdrževanje računalniške opreme v podjetjih. Njihovi strokovnjaki so izkušeni in usposobljeni za hitro odpravljanje morebitnih težav, kar zagotavlja nemoteno delovanje poslovnih procesov. Poleg tega nudijo tudi servis računalniške opreme, kar vključuje tako popravila kot tudi redno vzdrževanje.

Najem strežnikov in ostale opreme

Prav tako ponujajo tudi najem strežnikov ter ostale računalniške opreme (firewall, NAS, računalniki …). S svojo pestro ponudbo zadovoljujejo potrebe tako manjših kot večjih podjetij, pri čemer vedno stremijo k najboljšim rešitvam, ki so prilagojene specifičnim potrebam posamezne stranke.

Poudarek na varnosti

Ko je govora o IT omrežjih, se ne moremo izogniti vprašanju glede varnosti. Varovanje podatkov in omrežij je ključnega pomena za vsako podjetje. Pri IT-OPTI to dobro vedo, zato svojim strankam ponujajo celovite rešitve, ki vključujejo namestitev in konfiguracijo požarnih zidov (firewall), virtualnih zasebnih omrežij (VPN), segmentacijo omrežja ter vzpostavitev ustreznih gesel. Skozi svetovanje in izdelavo pravilnikov, povezanih z IT in varnostjo, strankam pomagajo vzpostaviti učinkovite protokole za varovanje njihovih podatkov. Temelj varnosti v IT-ju je ustrezen backup (varnostne kopije). IT-OPTI vam zagotovi izdelavo backup sheme, redno validacijo varnostnih kopij ter shranjevanje tako na lokaciji stranke kot na sekundarni lokaciji v Sloveniji ali EU. S tem zagotavljajo, da so podatki strank varno shranjeni in obenem dosegljivi v primeru kakršnega koli incidenta.

Nadzor v realnem času

Poleg vzdrževanja in varovanja opreme IT-OPTI ponuja tudi nadzor v realnem času, kar omogoča hitro in pravočasno ukrepanje v primeru kakršnih koli incidentov, kot so vdori v sistem ali pa težave z delovanjem opreme. Morebitne težave so na ta način identificirane in odpravljene takoj, kar minimizira morebitne posledice za poslovanje strank.

Arhiviranje e-pošte s programom Mailarhiv

In nenazadnje, posebna storitev, ki jo ponuja IT-OPTI, je arhiviranje e-pošte. S programom Mailarhiv lahko stranke arhivirajo svojo pošto že na strežniku. S tem prenesejo starejšo pošto v arhiv in sprostijo prostor v poštnem predalu na strežniku. Prva prednost tega je hitrejše iskanje po pojmih. Je pa arhiv shranjen na ločenem strežniku, kar zagotavlja njegovo dostopnost tudi v primeru izpada poštnega strežnika. Poleg tega je arhiviranje e-pošte skladno z GDPR in forenzičnimi preiskavami, kar pomeni, da je varno in zanesljivo. Podjetje IT-OPTI je pravi naslov, če stremite k varnemu, učinkovitemu in zanesljivemu IT-upravljanju. S svojimi strokovnjaki, celovitimi rešitvami in predanim pristopom zagotavljajo, da so podatki varni, omrežja pa vedno zanesljiva.

> DAS sistemi zagotavljajo neposredno povezavo z eno ali več napravami prek vmesnikov, kot so USB, Thunderbolt ali eSATA, kar omogoča visoko zmogljivost in nizke zakasnitve pri dostopu do podatkov.

IT-OPTI je tudi distributer za visokokakovostne NAS (Network Attached Storage) in DAS (Direct Attached Storage) sisteme blagovne znamke TerraMaster, ki predstavljajo ključne komponente za shranjevanje in upravljanje podatkov v sodobnih informacijskih okoljih. NAS sistemi omogočajo centralizirano shranjevanje podatkov v omrežju in enostaven dostop do datotek ter deljenje med več uporabniki ali napravami. Po drugi strani pa DAS sistemi zagotavljajo neposredno povezavo z eno ali več napravami prek vmesnikov, kot so USB, Thunderbolt ali eSATA, kar omogoča visoko zmogljivost in nizke zakasnitve pri dostopu do podatkov. TerraMaster se je izkazal kot vodilna blagovna znamka na tem področju, saj ponuja zanesljive in zmogljive sisteme, enostavne za uporabo, ki ustrezajo tako potrebam posameznikov kot tudi podjetij v različnih industrijah.

Več najdete na www.it-opti.com. (P.R.)

INTERVJU: Tomaž Kaluža, varnostni inženir pri podjetju Anni

Ukradli so nam gesla, kaj zdaj in kako se zaščititi?

O geslih, ki jih uporabljamo za dostop do svojih računov pri spletnih ponudnikih, se veliko govori. Mnogi vemo, da imamo prešibka gesla ali pa ista za dostop do različnih uporabniških računov. A kaj dejansko naredimo, da bi se zaščitili?

Ali se zares zavedamo, kakšna težava so lahko gesla? Kako nepridipravi pridobijo gesla uporabnikov? Kako se lahko zaščitimo in kaj lahko naredimo takrat, ko vemo, da je bilo naše geslo zlorabljeno? O tem smo se pogovarjali s Tomažem Kalužo, varnostnim inženirjem pri podjetju Anni, ki nam je pogosto na zanimiv način in s primeri predstavil, kako neprevidni znamo biti uporabniki spleta.

Dejstvo je, da si uporabniki neradi izmišljujejo nova in nova gesla ter jih ne spreminjajo redno. Se dovolj zavedajo, kakšna težava je to?

O tem se veliko piše in govori. Z malo domišljije si vsakdo lahko predstavlja, na kakšne načine vse je mogoče zlorabiti naše uporabniške račune. Če za primer vzamemo primarni e-poštni račun, s katerim smo registrirani v večino spletnih storitev in v katerem hranimo na primer žetone za večfaktorsko prijavo, je lahko škoda nepredstavljiva. Rekel bi, da se mnogi sicer zavedajo nevarnosti, pa vendar odlašajo in ne ukrepajo. Urejanja varnih gesel se moramo lotiti takoj, saj bo jutri lahko prepozno.

Zasebno morda ne skrbimo dovolj za varnost gesel. Je v poslovni rabi drugače?

V poslu marsikje že ustrezno skrbijo za primerno uporabo varnih gesel. V marsikaterem podjetju so že sprejeli tudi uporabo upraviteljev gesel. Ti uporabniki tudi v zasebnem življenju bolje razumejo pomen težave, ki jih prinašajo neprimerna gesla. Tisti, ki v poslovnih okoljih s tem nimajo stika, v večini sicer razumejo, da je to lahko težava, ampak si vse skupaj težje predstavljajo.
Varnost digitalnih računov je neotipljiva stvar. Da bi jo razumeli, pogosto potrebujemo malo več časa.

Imate kakšno primerjavo iz prakse, ki bi to postavila v bolj konkretno luč?

Seveda. Če izgubimo ključe svojega doma, ravnamo povsem drugače kot pri digitalnih računih. Zavedamo se, kaj vse hranimo doma, gre za otipljive stvari in hitro zamenjamo ključavnico. Ključa do nekega računa na spletu pa nimamo v rokah, je neotipljiv, tako kot stvari, ki so v spletnem računu shranjene. Zato jim ne posvečamo toliko pozornosti. V virtualnem svetu je ta predstava malo drugačna in ljudje s spremembo ključa, torej gesla, odlašajo.
Navedem lahko še eno primerjavo, ki še bolje ponazori razsežnost nevarnosti na spletu. Predstavljajmo si, da imamo isto geslo za več računov, kar lahko primerjamo z univerzalnim ključem, ki smo ga izgubili ali so nam ga ukradli. V realnem življenju bomo zamenjali vse ključavnice, ki jih ta ključ lahko odpira. Ne razumem najbolje, zakaj mnogi na spletu tega ne naredijo – torej zakaj ne spremenijo gesla vseh računov, pri katerih uporabljajo isto kombinacijo.
Zadnjič sem govoril z nekom, ki se mu je zdelo nečloveško, da bi si zapomnil množico gesel z 8, 12 ali 16 znaki. Jaz pa mislim, da ni tako, saj dejansko ni potrebe, da bi si zapomnili množico gesel. Potrebujemo sef z gesli (password sef) in eno dobro geslo za prijavo vanj ter drugi faktor avtentikacije, vseh ostalih gesel pa si ni treba zapomniti – in stvari postanejo enostavne.
Seveda pa lahko imamo v tem primeru veliko težavo, če kdo »razbije« to geslo in pridobi dostop do našega sefa in s tem do vseh gesel. Zato je pomembno, da je geslo, ki odpira vrata v svet vseh naših gesel, zares dobro in varno.

Kako pogosto pa je modro spreminjati gesla?

Ko izvajam izobraževanja in sprašujem, kdaj so tisti, ki sedijo v predavalnici, na zadnje zamenjali gesla, je veliko takšnih, ki jih sploh nikoli ne zamenjajo ali pa uporabljajo isto geslo v več storitvah. Ko jim predstavim, kakšno težavo lahko to predstavlja, hitro vidim kup zaskrbljenih obrazov. Gesla je pametno menjati enkrat letno, priporočam pa na pol leta. Z uporabo upravitelja gesel lahko to delamo tudi pogosteje, saj je zamenjava bolj enostavna.

Obstaja kakšno splošno pravilo, kako ustvariti varna gesla?

Gesla naj bodo dovolj dolga in kompleksna. Svetujem vsaj 16 znakov, gesla naj bodo sestavljena iz velikih, malih črk, številk in posebnih znakov. Za vsak uporabniški račun uporabimo svoje geslo. Lahko uporabimo hudomušne stavke z uporabo narečnih besed, ki niso v slovarjih, a si jih obenem enostavno zapomnimo. Najvarnejša so seveda naključno generirana gesla iz velikega števila znakov. Pomembno je, da ne zapisujemo gesel v datoteke in jih ne delimo. Z uporabo upraviteljev gesel je vse našteto zelo enostavno.

Kaj pa je sicer ključna težava upravljanja gesel?

Povprečni uporabnik v EU ima skoraj 100 uporabniških računov, mnogi jih imajo veliko več. Takšno množico dobrih gesel pa si človek težko zapomni. Nekateri za to uporabljajo sisteme, ki niso ravno najprimernejši – v geslu spremenijo nekaj znakov, mogoče kakšno besedo. Z uporabo velike procesorske moči, ki je na voljo vsakomur, je možno 8 znakov dolgo geslo, sestavljeno iz malih, velikih črk, številk in posebnih znakov, razbiti v nekaj minutah. Kritična je lahko tudi varnost hrambe gesel ali zgoščenih vrednosti pri upravljalcu storitev, saj lahko nepridiprav ukrade celotno bazo le teh in jo proda na temnem spletu. Če uporabnik takšno geslo uporabi pri več računih, je to velik problem. Januarja letos so odkrili tako imenovano »mother of all breaches« bazo s 26 miliiardami uporabniških gesel. Je vaše lahko v tej bazi?

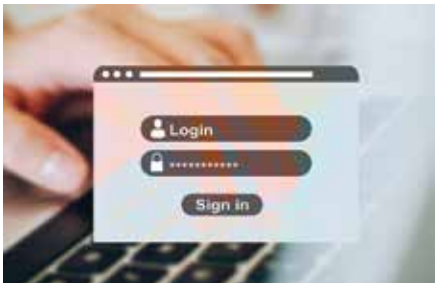
Če geslo, ki je v takšni bazi, uporabljamo za dostop do več računov, morda celo poslovnih, imamo lahko veliko težavo. Nepridipravi tako pridobijo dostop do poslovnih sistemov in podatkov, ki jih lahko izkoristijo in povzročijo nepredstavljivo škodo.

Kako nepridipravi najpogosteje pridejo do gesel uporabnikov?

Taktik, tehnik in procedur za pridobitev gesla uporabnika je veliko. Nepridipravi so zelo iznajdljivi in vsak dan odkrivajo nove načine. Opažamo pa, da je v večini primerov, vsaj v poslovnem svetu, za krajo poverilnic uporabljeno ribarjenje, pa tudi ponovna uporaba gesel, ki so jih hekerji že odkrili. Pogosto je geslo uporabnika za poslovni račun (npr. Office 365) isto kot geslo nekaj njegovih privatnih računov, ki so že bili zlorabljeni. Nezanemarljivo pa je tudi število primerov, kjer so uporabniki geslo enostavno povedali nepridipravu – gre za socialni inženiring.

Bili so primeri, ko so nepridipravi klicali v podjetje in se predstavili, da so iz uporabniške podpore Microsofta, ti pa so jim izdali geslo. Tudi na to moramo biti pozorni. Smo manjša država in naš jezik je malo bolj kompleksen, tako da je tega mogoče pri nas malo manj, ampak če je napadalec slovensko govoreči, je to zelo enostavno.

Danes je z uporabo orodij z umetno inteligenco že možen »deep fake«, tako da je tudi tujcem vse lažje posneti neko besedilo v slovenskem jeziku. Za zdaj to ni povsem enostavno, ampak se je tudi to v našem okolju že zgodilo. Danes umetna inteligenca vseeno še ni tako pametna, kot bi si včasih radi predstavljali, a to se bo le še razvijalo in v prihodnosti bo tudi to, kar smo zgoraj omenili, lažje narediti in pretentati uporabnika.



Kaj lahko naredimo enkrat, ko vemo, da je bilo naše geslo zlorabljeno?

Če gre za poslovni uporabniški račun, najprej o tem obvestimo osebo, odgovorno za varnost ali IT oddelek in sledimo njihovim navodilom. V primeru osebnega računa takoj zamenjamo geslo, preverimo varnostne nastavitve računa, kjer odstranimo zaupanja vredne naprave in omogočimo večfaktorsko prijavo. V primeru zlorabe e-poštnega računa temeljito preverimo vse nastavitve, kot je na primer preusmerjanje/posredovanje vseh poštnih sporočil. To mora biti tudi alarm in skrajni čas, da uredimo dostope do vseh ostalih računov.

Smo uporabniki, ko se nam enkrat to zgodi, v prihodnje bolj pozorni ali nam ni nič bolj mar kot pred tem?

Veliko je odvisno od škode, ki smo jo utrpeli. Nekaj časa smo seveda prestrašeni in bolj pozorni, potem dogodek pogosto pozabimo in nadaljujemo z ustaljeno prakso. Škoda je žal lahko zelo velika.

Kakšna so vaša priporočila, kako v podjetju in tudi zasebno poskrbeti za varna gesla?

V podjetju je pomembno, da so v sistemu nastavljene primerne politike gesel (dovolj dolga in kompleksna gesla, onemogočeno ponavljanje istih gesel, po drugi strani pa ne prepogosto menjavanje), ločeni upravljavski računi, onemogočeni ranljivi avtentikacijski protokoli in podobno. Priporočam uporabo upravitelja gesel, ki močno olajša varno rabo, primerno shranjevanje in deljenje poverilnic, kjer je omogočeno sledenje uporabe in morebitnih sprememb, preverjanje varnosti, ponavljanja gesel, morebitnih vdorov in veliko ostalih poročil. Enako velja za zasebna gesla. Dobri upravitelji gesel stanejo veliko manj kot nas lahko stanejo morebitne zlorabe. Zaščitite sebe in družinske člane, da ne postanejo žrtve spletnih zlorab.

V kolikšni meri je pri varnosti podjetja na spletu pomembno to, da ima podjetje preizkušeno storitev upravljanja gesel?

V primeru, da napadalec pridobi veljavno geslo, nam pri preprečevanju zlorabe ne pomaga nobeno orodje. Na voljo je veliko odprtokodnih in brezplačnih orodij za varno hrambo gesel, vendar vsa niso najprimernejša za uporabo v poslovnem okolju. Pomemben je tudi varnostni model kriptiranja sefov in prenosa gesel pri vpisovanju v storitve.

Lahko omenimo še možnost zagotavljanja varnosti hrambe sefov v lastnem okolju podjetja, a je to pogosto prevelik zalogaj, zato je hramba pri zunanjem ponudniku primernejša.

Seveda moramo vedeti, da nobena storitev ni 100 % varna, prav tako ne upravitelj gesel. Če pa poskrbimo za stvari, ki sva jih midva tu omenila, bo skoraj nemogoče priti do gesel. Vse se da »pohekat«, a če pa je varnostni model upravitelja gesel dober, bo to veliko težje.

Lahko pa na primer uporabljamo dobrega upravitelja, a imamo premalo kompleksno glavno geslo. Za vse vidike moramo kar najbolje poskrbeti.

Kakšni pa so trendi na tem področju?

V ospredje vse bolj prihaja uporaba tako imenovanih "passkeys", saj nima toliko ranljivosti, kot jih imajo klasična gesla. To je tehnologija, ki temelji na uporabi javnih ključev, ki jih ima ponudnik, in privatnih ključev, ki so shranjeni na uporabnikovi napravi ali recimo password sefu oziroma sefu z gesli (ki ga odklenemo s prstnim odtisom, prepoznavo obraza, dobro PIN kodo). Le naprava, ki ključ hrani, ima možnost dostopa do našega uporabniškega računa. Zato je možnost zlorabe, manjša. Prav tako si s passkeys ni potrebno več izmišljati in zapomniti kompleksnih gesel, hekerjem pa je onemogočena kraja baz gesel ali njihovih zgoščenih vrednosti, shranjenih na strežnikih ponudnikov storitev. Sodobni upravitelji gesel, kot je na primer 1Password, že omogočajo uporabo passkeys. (P.R.)

ADM ADRIA D.O.O.

Zmanjšajte tveganja za svojo strategijo hibridnega oblaka s Foglight® by Quest®

KAKO LAHKO ZMANJŠATE KOMPLEKSNOST SVOJEGA OKOLJA IN NAREDITE PREHOD NA HIBRIDNO INFRASTRUKTURO MANJ BOLEČ?

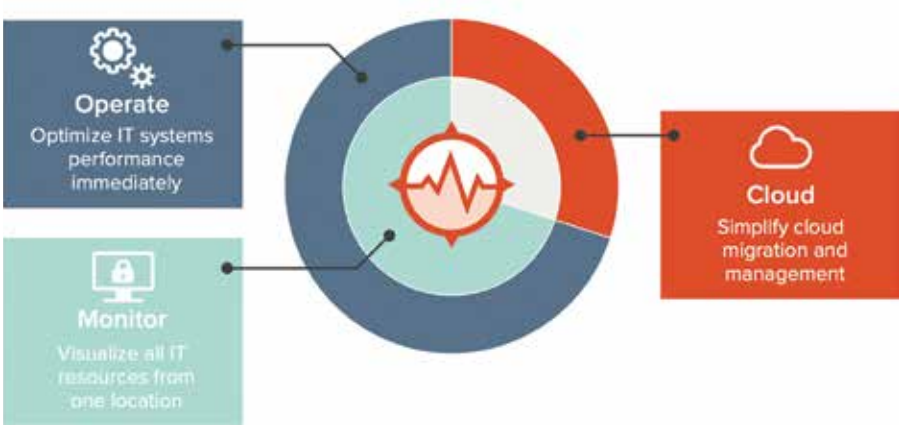
SPREMLJANJE, PRIMERJALNA ANALIZA IN VARNOSTNO KOPIRANJE

Glede na današnje možnosti javnega in zasebnega oblaka je premikanje podatkov in delovnih obremenitev v oblak trend, ki ne kaže znakov upočasnitve. Po Gartnerju in drugih virih naj bi selitev v oblak pospešilo obdobje po pandemiji. Za vodje IT je uvedba hibridne infrastrukture v oblaku za podatkovne platforme smiselna, saj iščejo načine za znižanje stroškov in odstranitev bremena lastne strojne opreme. Toda prehod na infrastrukturo v več oblakih – morda z mešanico sistemov na mestu uporabe – prinaša tveganja, ki lahko hitro izničijo morebitne koristi.

Vodje IT morajo zagotavljati, da so na voljo viri in orodja za ohranjanje visoke kakovosti storitev, medtem ko si prizadevajo zmanjšati stroške in ublažiti tveganja, kot so kršitve podatkov in neskladnost. Upravljanju je treba nameniti stalno pozornost podatkovnih baz, hipervizorjev in virtualizacije itd., kakor tudi komunikaciji in procesom, ki jih zahteva hibridni IT. Ne glede na to, kako ste vi in vaša ekipa strukturirali hibridne operacije za svojo organizacijo, je raznolik nabor

ADM - Adria d.o.o.
Mariborska cesta 86
3000 Celje

+386 59 251 955
info@adm-adria.eu
www.adm-adria.si



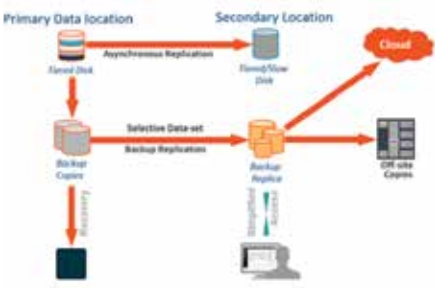
veščin v IT nujen. Izzivi, ki lahko ogrozijo vašo hibridno strategijo IT, vključujejo:

- nepoznavanje novih platform za baze podatkov,
- pomanjkanje izkušenj pri spremljanju delovanja in diagnostiki,
- pomanjkanje znanja ali zavedanja o optimizaciji delovne obremenitve in modeliranju stroškov v oblaku,
- nezmožnost samozavestnega zagovarjanja migracije v oblak.

Ključni cilj strategije hibridnega oblaka bi moralo biti zmanjšanje presenečenj in težav ter s tem zmanjšanje operativnih stroškov.

Z zgodnjim odkrivanjem težav z infrastrukturo in zbirkami podatkov ter odpravljanjem težav, ko so odkrite, lahko proaktivno obravnavate komponente infrastrukture, ki bodo na koncu zahtevale manj pozornosti in odpravljanja težav. Nižji stroški in višja raven storitev so rezultati, ki bi jih pozdravil vsak IT vodja.

Foglight® by Quest® je tako najširša in najgloblja rešitev za spremljanje in optimizacijo za hibridna podjetja. Z Foglightom lahko zmanjšate kompleksnost svojega okolja in sprostite čas



osebja, tako da v celoti sprejmete digitalno preobrazbo.

Povrnete lahko premalo uporabljene vire – prihranite stroške oblaka in povečate zmogljivost obstoječih sistemov. Natančneje lahko napoveste prihodnje stroške. Poleg tega lahko predvidite prihodnja ozka grla in izpade, preden se zgodijo, ter proaktivno vplivate na največji čas delovanja in razpoložljivost sistema.

> Foglight® by Quest®
> je najširša in najgloblja rešitev
> za spremljanje in optimizacijo za
> hibridna podjetja.

Foglight® by Quest® je edinstven tako po širini dosega kot po globini zbiranja podatkov za reševanje problemov.

V idealnem okolju bi imele organizacije, ki se lotevajo projekta migracije v hibridni oblak, na voljo orodja za merjenje in modeliranje stroškov in učinkovitosti delovnih obremenitev v širokem naboru lokalnih infrastruktur in infrastruktur v oblaku. Ta primerjalna analiza in testiranje pomagata določiti dodelitve virov in ravni storitev v oblaku pred selitvijo, tako da na tej poti ni presenečenj.

S pomočjo Foglighta in razumevanjem orodja lahko izvedete vaše migracije podatkov brez bolečin in si tako zagotovite prehod na nove tehnologije brez tveganj. Za več informacij obiščete spletno stran www.adm-adria.eu. (P.R.)

ZASEBNO 5G OMREŽJE

T-2 z inovativno 5G rešitvijo pionir na področju pametnih tovarn

T-2 je vzpostavil zasebni 5G SA sistem in je s tem razvil rešitev, ki jo že lahko ponudi trgu. 5G tehnologija bo v prihodnosti ključna za digitalizacijo in avtomatizacijo tovarn.

Brezžična povezljivost na najvišji ravni zanesljivosti in varnosti z zasebnim 5G omrežjem je postala realnost in podjetje T-2 je svojo rešitev uspešno lansiral v sodelovanju s podjetjem CABLEX-T. Že v svoji prvi postavitvi sistema je 5G tehnologija omogočila prenos podatkov v zahtevnem proizvodnem okolju, kjer ostalim brezžičnim tehnologijam to ni uspelo. S tem je zasebni 5G SA sistem izkazal velik potencial za reševanje obstoječih težav povezljivosti naprav v slovenskih proizvodnih obratih, ponudnik T-2 pa lahko zdaj to rešitev kot prvi v Sloveniji ponudi trgu.

PREDNOSTI ZASEBNEGA 5G SA (STANDALONE) SISTEMA ZA INDUSTRIJO:

Dodatno izboljša izkoriščenost proizvodnih naprav oziroma zviša OEE (skupna učinkovitost).

- Z dodajanjem senzorjev preko 5G omrežja nadgradi oz. digitalizira obstoječe analogne stroje, s tem prihrani na investiciji za nove in jih enakovredno vključi v industrijske MES/ERP sisteme.
- Poveča produktivnost proizvodnje, hitrost analitike in odzivanja na trg, s tem pa viša konkurenčno prednost in potencira dobičke.
- Uvaja analitiko v realnem času in pravočasno naročanje, kar omogoča boljše upravljanje skladišč, optimizacijo logističnih postopkov, manjšanje skladiščnih zalog in s tem povečanje finančnih učinkov podjetja.
- Preko senzorjev, nameščenih na različnih nivojih procesa, uvaja hitro zaznavanje in odpravljanje napak. In ne le to – ko enkrat zbere dovolj proizvodnih podatkov, lahko z veliko verjetnostjo celo predvidi napake.
- Preko senzorjev v realnem času zbira tehnološke podatke in optimizira tehnološki proces.
- Industrija si s takšnimi rešitvami tudi dviguje ceno za primer prodaje oz. nakupa s strani potencialnih vlagateljev.

Bolje kot kabel, bolje kot WiFi

Podjetje T-2 kot pionir na slovenskem trgu odpravlja potrebo po kabelskih povezavah v industriji. S tem omogoča učinkovitejšo uporabo prostora in občutno cenejše redno vzdrževanje proizvodnih obratov. Z uporabo 5G SA (Standalone) sistema za pametne tovarne upravljalcem tovarn omogoča neodvisnost od zunanjih omrežij in najvišjo raven kibernetske varnosti, saj je omrežje popolnoma samostojno. Rešitev presega hitrost in zanesljivost klasičnih kabelskih povezav v industriji. Hkrati 5G omrežje omogoča večjo mobilnost, nižje stroške vzdrževanja in boljšo skalabilnost – lažje širjenje omrežja ob spreminjajočih potrebah proizvodnje.

Nadalje se lahko vprašamo, zakaj izzivov ne bi reševali z WiFi omrežjem? Razlogov vprid 5G SA je več.

5G omrežja ponujajo visoke hitrosti v gigabitnem obsegu, medtem ko se hitrosti WiFi lahko razlikujejo glede na usmerjevalnik in razdaljo od dostopne točke. Pri 5G lahko računamo na veliko nižjo zakasnitev, kar je zelo pomembno za aplikacije, ki delujejo v realnem času, navidezno resničnost, avtonomna vozila v tovarnah in podobno. 5G omrežje je bolj zanesljivo in varno, saj vključuje močnejše šifriranje in protokole za preverjanje pristnosti ter avtentikacijo. Zaradi vsega naštetega je idealno za IoT in industrijo 4.0.

Najvišja raven varnosti in enostavna namestitev

Ker postavitev 5G SA v nasprotju od 5G NSA ni odvisna od obstoječih omrežij, omogoča večjo prilagodljivost in možnost optimizacije, pa tudi manjšo zakasnitev ter manjše tveganje za varnostne napade in boljšo zaščito podatkov, saj ni povezan z obstoječimi 4G omrežji.

Rešitev torej nadgrajuje tradicionalne varnostne mehanizme z integracijo on-premise (na mestu uporabe) strojne infrastrukture, ki deluje v izoliranih omrežjih. S tem je zagotovljena najvišja raven kibernetske varnosti preko šifriranja end-to-end, robustnih firewalls (požarnih zidov), in standardiziranih protokolov za varno komunikacijo. Tveganje zunanjih vdorov je minimalno. Omogoča tudi boljši nadzor nad uporabniškimi napravami ter preprečevanje dostopa neželenim in nevarnim napravam, ki so povezane v omrežje.

Omrežje 5G SA tudi ne zahteva zapletenega postopka namestitve. Sistem je prednastavljen in že konfiguriran ter pripravljen za uporabo. Poleg tega je na kolesih in omogoča hitro implementacijo, enostavno premikanje in postavitev na različnih lokacijah. Ker je sistem prednastavljen, lahko pričakujete manjše stroške ter manj možnosti za morebitne napake. Ko potrebujete nove funkcionalnosti, pa je enostavno nadgradljiv.

Več informacij najdete na spletni strani www.t-2.net. (P.R.)

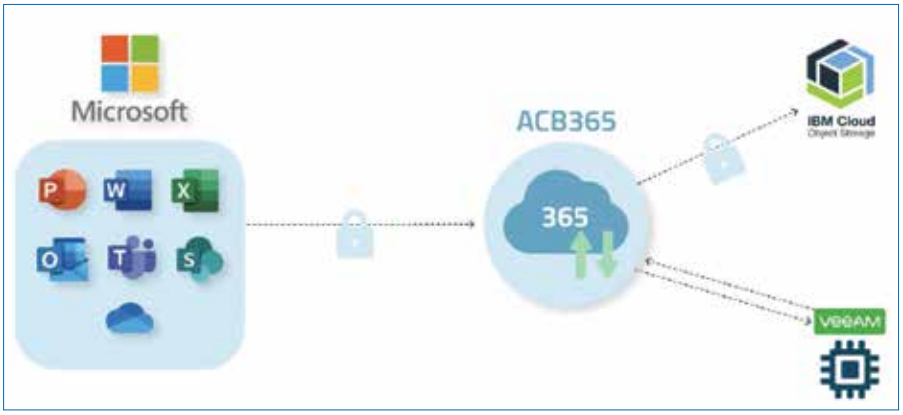
www.t-2.net

IBM ANYCLOUD BACKUP FOR 365

Kako zaščititi podatke v okolju Microsoft 365?

Podatki obenem predstavljajo življenje in potencialno pogubo podjetja. Z njimi lahko poslujemo uspešno, brez njih pa se naša zgodba lahko zaključi z le nekaj kliki kibernetskih nepridipravov ali celo nespretnih rok lastnih zaposlenih.

Ni dneva, ko se vodilni v podjetjih ne bi vprašali, kaj lahko še storijo za varstvo kritičnih podatkov. Največja podjetja z vsakim novim preventivnim mehanizmom zmanjšajo možnost izgube podatkov in večmilijonsko odpravljanje posledic. Vendar najti pravi odgovor na kibernetske in ostale grožnje, ki pretijo podatkom, ni enostavno. V iskanju prave rešitve so se združili IBM, Microsoft, Anycloud in Veeam ter pripravili rešitev Anycloud Backup for 365 za neoporečnost podatkov v okolju Microsoft 365. Storitev je sklenjena s fiksno mesečno ceno, tako da lahko uporabnik enostavno načrtuje svoje stroške, ne da bi bil presenečen, če se bo količina podatkov povečala.



IBM Anycloud Backup for 365 - močno šifriranje, granularna obnovitev in 10-letna hramba

Nepridipravi so vam vdrli v mrežo in z ransomware virusom ohromili podjetje. Preostane vam, da ugodite njihovim zahtevam in upate, da bodo osvobodili vaše podatke in sisteme, ali pa jim že pred tem vrzite polena pod tipkovnice in vzpostavite celovito rešitev AnyCloud Backup for 365, s katero si boste povrnili vse podatke in vzpostavili normalno delovanje v najkrajšem času.

Kako deluje IBM Anycloud Backup for 365?

Okolje Microsoft 365 je močno orodje za produktivnost in komunikacijo. Lahko si predstavljate količine podatkov, ki vsakodnevno krožijo s pomočjo Microsoftovih orodij (Teams, OneDrive, Outlook …). Njihova varnost bi morala biti prioriteta številka ena.

Anycloud Backup for 365 to stori z varnostnim kopiranjem v oblak IBM Cloud. Gre za mrežo 18 podatkovnih centrov v 13 državah. Njihova minimalna klasifikacija je Tier 3, kar pomeni, da s pomočjo naprednih sistemov za redundanco zagotavljajo čas delovanja 99,982 % na leto. To je prva stopnička do pridobivanja zaupanja strank. Druga in tretja sta certifikata ISO 27001 in ISAE 3000 ter članstvo v združenju CSA (angl. Cloud Security Alliance).

Lokacijo podatkovnega centra izbere uporabnik. Podatki so ob kopiranju razdeljeni v ločena fizična okolja, tako so kopije vedno ločene od produkcijskih podatkov, kar se je izkazalo za zanesljivo zaščito pred izsiljevalskimi programi. Poleg tega Anycloud Backup ustvari varnostno kopijo, v kateri se podatki okolja Microsofta 365 in programov Exchange, SharePoint, OneDrive, Teams ne morejo spreminjati, prepisati ali izbrisati.

Med prenosom in tudi med samo hrambo pa podatke varuje močno AES256-bitno šifriranje, ki preprečuje (ne)namerne izbrise ali spremembe.

Celovita rešitev za prenos podatkov iz oblaka v oblak

Anycloud Backup for 365 je ločen na tri portale. Sistemski administrator v portalu za upravljanje določi pogostost varnostnih kopij. Te se lahko izvajajo večkrat dnevno, tedensko, mesečno ali letno. Podatki se hranijo do 10 let, Anycloud pa pripravlja tudi možnost 25-letne varne hrambe. Kreiranje varnostne kopije celotnega okolja traja le nekaj minut, na voljo pa so tudi poročila za vsako kopijo ali postopek obnovitve, vključno s podatki, kdo je zahteval varnostno kopijo/obnovitev in kaj ter kdaj so se podatki obnovili. Sistemski administrator lahko obnovi celotne mape ali pa le posamezne datoteke.

Končni uporabniki oziroma zaposleni si lahko sami obnovijo e-poštna sporočila (na prvotno ali drugo lokacijo) ali OneDrive datoteke. Anycloud Backup omogoča tudi popoln izbris podatkov določenega uporabnika v skladu z uredbo GDPR. Ker grožnje lahko izvirajo tudi znotraj podjetja, Anycloud zagotavlja 30-dnevno obdobje, v katerem si lahko v celoti obnovite podatke.

Zavarujte svoje podatke

Anycloud Backup for 365 se bo prilagodil vašim potrebam, ne glede na to, ali vodite majhno podjetje ali korporacijo. Vaši podatki bodo na varnem v IBM podatkovnih centrih, fizično ločeni od okolja Microsoft 365 in sistemov vašega podjetja. Zaprite vrata nepridipravom in poskrbite, da bodo vaši podatki služili samo vam.

Več na https://cloud.ibm.com/catalog/services/anycloud-backup-for-365#about. (P.R.)

ALSO TECHNOLOGY IN HUAWEI SOLARNE REŠITVE

Inovacije v svetu sončne energije za domačo uporabo

Vse bolj se zavedamo pomena obnovljivih virov energije in Huawei predstavlja na tem področju vrhunec inovacij s svojo linijo izdelkov FusionSolar za stanovanjske objekte.

S celovito rešitvijo, ki združuje optimizatorje in sisteme za shranjevanje energije, Huawei postavlja nove standarde v industriji sončne energije.

Inovativne rešitve fotovoltaičnih sistemov

V zadnjih letih narašča povpraševanje po čistih in obnovljivih virih energije. Zaradi skrbi glede podnebnih sprememb in izčrpavanja fosilnih goriv, se vse več posameznikov in podjetij odloča za sončno energijo kot smiselno alternativo. Med vodilnimi podjetji v sektorju sončne energije se je Huawei izkazal kot ključni igralec s svojimi inovativnimi rešitvami fotovoltaičnih (PV) sistemov. Napredne tehnologije in koristi, ki jih prinaša Huawei, so vrhunska izbira za vse tiste, ki želijo izkoristiti prednosti sončne energije.

Eden izmed ključnih elementov Huaweijevih FusionSolar je njihova napredna pametna tehnologija PV. Omogoča brezhibno integracijo proizvodnje, shranjevanja in porabe sončne energije. Z uporabo pametnih rešitev PV Huawei lahko uporabniki učinkovito upravljajo in optimizirajo svojo porabo energije, kar zagotavlja maksimalno učinkovitost in prihranke. S pomočjo inteligentnih sistemov za nadzor in upravljanje Huawei uporabnikom omogoča, da oddaljeno spremljajo svoje sončne sisteme in na podlagi vzorcev porabe energije izvajajo prilagoditve v realnem času. Rešitve FusionSolar so tudi sinonim za zanesljivost in varnost. Njihovi pretvorniki (inverterji) visoke učinkovitosti zagotavljajo večjo pretvorbo sončne energije v uporabno elektriko. Poleg tega se ti pretvorniki ponašajo z širokim razponom napetosti, ki omogoča delovanje v različnih vremenskih pogojih in zagotavlja dosledne zmogljivosti. Z vgrajenimi mehanizmi za zaščito, kot so zaščita pred prenapetostjo in prekomernim tokom, Huawei daje prednost varnosti in uporabnikom zagotavljaja miren spanec.

Zavezanost Huaweija raziskavam in razvoju je še en razlog za njihovo priljubljenost in razširjenost. Podjetje vlaga pomembne vire v razvoj in izboljšanje svojih rešitev PV ter nenehno premika meje inovacij. Inženirji in raziskovalci Huaweija si prizadevajo izboljšati učinkovitost, trajnost in zmogljivost svojih izdelkov. Rešitve Huawei FusionSolar so najsodobnejše in najkonkurenčnejše na trgu.

Razširljivost in prilagodljivost

Huaweijeve rešitve PV so zasnovane z mislijo na razširljivost in prilagodljivost. Ne glede na to, ali ste domači uporabnik, ki želi napajati svoj dom, ali veliko komercialno podjetje s širokimi energetskimi zahtevami, Huawei ponuja rešitve, ki ustrezajo vašim potrebam. Z modularnimi oblikami in enostavnimi postopki namestitve se Huaweijeve rešitve prilagodijo različnim aplikacijam. Zaradi razširljivosti in prilagodljivosti je Huawei idealna izbira za posameznike in podjetja, ki želijo vključiti sončno energijo v svoje operacije brez motenj.

Huawei s svojo linijo izdelkov FusionSolar za stanovanjske objekte predstavlja vrhunec inovacij. S celovito rešitvijo, ki združuje napredne optimizatorje in sisteme za shranjevanje energije, postavlja nove standarde v industriji sončne energije. Z izbiro Huaweijevih rešitev PV lahko prispevamo k trajnostni in bolj zeleni prihodnosti ter uživamo v koristih učinkovite in stroškovno učinkovite sončne energije.

Integratorjem solarnih rešitev je z letošnjim letom na voljo lokalni distributer ALSO s celovito ponudbo in podporo, kar končnim uporabnikom prinaša dodatne prednosti in partnerja, ki jim je vedno na voljo.

Več informacij na bit.ly/also-huawei. (P.R.)

ALSO Technology Ljubljana, d.o.o.

Ukmarjeva ulica 2, 1000 Ljubljana
info.si@also.com
+386 1 4205 506

TELEMACH

Interne IT ekipe same težko skrbijo za kibernetsko varnost

Zagotavljanje kibernetske varnosti je postalo eden izmed največjih izzivov za organizacije vseh velikosti. Kibernetske grožnje postajajo vse bolj kompleksne in interne IT ekipe so jim težko kos.

Čeprav so interne IT ekipe dolgo časa uspešno skrbele za varnost naprav in omrežij, se je s pojavom vse bolj kompleksnih in prefinjenih kibernetskih groženj pokazalo, da samostojno ne zmorejo več zagotavljati zadostne ravni varnosti. Vzrokov za to je več, a ključna težava je v hitro razvijajočih se tehnikah napadov, ki pogosto presegajo znanje in izkušnje internih ekip.

Zakaj kibernetsko varnost zaupati zunanjim strokovnjakom?

Zaradi zgoraj navedenih razlogov organizacije vse pogosteje kibernetsko varnost prepuščajo zunanjim izvajalcem (outsourcing). S tem pristopom organizacije, ki bi se rade zaščitile pred kibernetskimi grožnjami, izboljšajo svoje možnosti za preprečevanje in odkrivanje napadov, zmanjšajo tveganja ter povečajo učinkovitost svojih varnostnih ukrepov.

Podjetja imajo največkrat le nekaj IT strokovnjakov, odvisno od velikosti same organizacije. Ti pogosto niso ozko usmerjeni zgolj na področje varnosti. S tem, ko podjetja kibernetsko varnost prepustijo zunanjim izvajalcem, pridobijo dostop do širokega spektra strokovnjakov s specializiranim znanjem in izkušnjami na tem področju ter z obsežnim znanjem o najnovejših kibernetskih grožnjah in naprednih obrambnih strategijah, ki jih interne ekipe pogosto nimajo.

Ena izmed najboljših rešitev je MDR

Prav zato se izkaže, da je storitev MDR (Managed Detection and Response) ena izmed najboljših rešitev za organizacije, ki iščejo zanesljiv in celovit pristop k varovanju svojih sistemov. MDR storitve združujejo napredno tehnologijo, strokovno znanje in nadzor 24/7, vse to pa omogoča hitro odkrivanje, analizo in odzivanje na kibernetske napade v realnem času.

Ker je kibernetska varnost ena izmed ključnih prednostnih nalog za organizacije v vseh sektorjih je pomembno, da te prepoznajo svoje omejitve in se obrnejo k zunanjim strokovnjakom, ki lahko nudijo boljše, specializirane rešitve. Z izbiro pravega zunanjega partnerja tako organizacije dosežejo višjo raven varnosti ter bolje obvladujejo kibernetska tveganja.

V primerjavi med »vedno na voljo MDR storitvami«, ki jih ponuja Telemach, in manjšimi SOC-i (varnostni operativnimi centri), kot jih ponujajo nekateri operaterji, obstajajo pomembne razlike:

Obseg storitev in zmogljivosti: Vedno na voljo MDR storitve običajno ponujajo celovito paleto storitev, ki vključujejo stalni nadzor, analizo groženj, odziv na incidente, forenzično analizo in svetovanje. Manjši SOC-i pa običajno nudijo osnovno raven storitev.

Specializirano znanje in izkušnje: Ponudniki MDR storitev imajo vedno na voljo dostop do vrhunskih strokovnjakov s specializiranim znanjem in izkušnjami na področju kibernetske varnosti. Manjši SOC-i pogosto nimajo enake stopnje specializiranega znanja in izkušenj.

Nadgradnje in prilagodljivost: Vedno na voljo MDR storitve običajno vključujejo redne nadgradnje in prilagodljivost, ki omogočajo hitro prilagajanje spremembam. Manjši SOC-i navadno nimajo enake stopnje prilagodljivosti ali hitrosti.

Storitvena podpora in odzivni časi: Pri vedno na voljo MDR storitvah so običajno zagotovljeni hitri odzivni časi v primeru incidentov in visoka stopnja storitvene podpore, medtem ko se manjši SOC-i s tem ne morejo pohvaliti v tolikšni meri.

Ni vseeno, katerega partnerja izberete

Izredno pomembno je tudi to, da organizacije izberejo partnerja, ki ima potrebno znanje, izkušnje in tehnične zmogljivosti. Šele pravilna izbira partnerja zagotavlja najboljšo možno zaščito, obenem pa organizacijam in internim ekipam omogoča, da se osredotočijo na svoje osnovno poslovanje – medtem zunanji strokovnjaki za kibernetsko varnost prevzamejo odgovornost za varovanje njihovih informacijskih sistemov.

Tudi pri kibernetski varnosti je namreč pomembna celovitost, saj polovično delo prinaša tudi polovične rezultate, kar je lahko, ko govorimo o kibernetski varnosti, za podjetje tudi usodno ali pa vsaj zelo boleče.

Zato pri Telemach Slovenija ponujajo celovito rešitev Sophos MDR, ki je najbolje ocenjena MDR rešitev s strani G2 ocenjevalcev. O njej lahko več preberete tudi v naslednjem članku.

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

telemach

SOPHOS MDR

Preverite, zakaj vas Sophos MDR najbolje ščiti pred računalniškimi grožnjami

Vsakodnevni avtomatski ali ciljani kibernetski napadi na podjetja po svetu so že nekaj časa stalnica in žal so tarče v vse večji meri tudi slovenska podjetja.

Varuje že več kot 20.000 podjetij

Zaradi pomanjkanja računalniških strokovnjakov za varnost so podjetja tako primorana iskati zunanje strokovnjake ali podjetja, ki so specializirana za računalniško varnost in nudijo MDR storitev (Managed Detection and Response). Tudi podjetja, ki že imajo svoj lasten SOC oddelek, se srečujejo s težavami zaradi preobremenjenosti in pomanjkanja kadra.

Zato je podjetje Sophos, ki s svojimi produkti za kibernetsko varnost varuje podjetja po vsem svetu že več kot 30 let, pred 3 leti predstavilo svojo MDR storitev, ki jo je v tem času začelo uporabljati že več kot 20.000 podjetij. To število pomeni, da je Sophos MDR najbolj razširjena MDR storitev na svetu in ne samo to, ima tudi najboljšo oceno (Gartner Peer Review) s strani uporabnikov med vsemi MDR storitvami. Prav tako je najbolje ocenjena MDR storitev s strani G2 ocenjevalcev, kar postavlja Sophos MDR pred konkurenco in kot logično izbiro.

Povprečen čas Sophos MDR storitve od najdbe do odstranitve grožnje je 38 minut, kar je mnogo manj od povprečnega časa pri uporabnikih z lastnim SOC centrom.

Kaj je Sophos MDR storitev

Storitev Sophos MDR združuje človeško strokovno analizo in napredne tehnologije umetne inteligence za hitro in samodejno odkrivanje groženj. Podjetjem nudi možnost stalnega nadzora, odkrivanja in odzivanja na računalniške grožnje, kar izvajajo strokovnjaki podjetja Sophos, in to neprekinjeno vse dni v letu, brez izjem. Podjetja se lahko ali popolnoma zanesejo na Sophos strokovnjake in tako nadomestijo lasten SOC ali pa Sophos MDR dopolnjuje in nadgrajuje obstoječi SOC oddelek v podjetju. Zanimiva za podjetja je tudi odškodnina v višini do 1 milijona ameriških dolarjev v primeru vdora v podjetje in hkratne uporabe Sophos MDR Complete storitev.

Povezljivost z drugimi varnostnimi produkti

Sophos MDR kot edini ponudnik ponuja možnost branja podatkov iz produktov drugih proizvajalcev varnostnih storitev, kar pomeni natančnejše spremljanje varnostnih dogodkov in še hitrejše odzivanje na grožnje. Sophos MDR ima tako možnost branja podatkov in telemetrije proizvajalcev, kot so na primer: Microsoft, AWS, CrowdStrike, Veeam, Cisco, Palo Alto Networks, Fortinet, Check Point, Rapid7, Google Workspace, Okta, Darktrace, Mimecast in še mnogo drugih proizvajalcev.

Sophos Forum 2024

Če bi želeli izvedeti več o Sophos MDR storitvi in vseh ostalih Sophos produktih, vas vabimo na Sophos Forum seminar 2024, ki bo potekal 23. aprila v Hotelu Šport Otočec, kjer vam bodo poleg Sophos produktov in novosti predstavili še primere dobre prakse. Ob prijetnem druženju si boste lahko izmenjali mnenja in izkušnje. Če bi se želeli udeležiti srečanja, to sporočite na el. naslov: slovenija@sophos.si najkasneje do 21.aprila. Udeležba je brezplačna. (P.R.)

PAM: PRIVILEGED ACCESS MANAGEMENT

PAM rešitve za privilegirane dostope do kritičnih virov v organizacijah

PAM rešitve se uporabljajo za upravljanje, nadzor in sledenje privilegiranemu dostopu uporabnikov do kritičnih virov, kot so strežniki, podatkovne baze, omrežna oprema ... v sodobnih organizacijah.

Upravljanje privilegiranega dostopa postaja glavna prednostna naloga za zagotavljanje kibernetske varnosti. Zlonamerni uporabnik z dostopom do skrbniškega računa lahko organizaciji povzroči veliko večjo škodo v primerjavi z običajnim osebjem z omejenimi pravicami. Zagotavljanje varnosti privilegiranega dostopa je prefinjena naloga; tega ni mogoče doseči z zanašanjem izključno na skupne pristope k zaščiti poverilnic, saj zahteva specializirane rešitve, kot je Axidian PAM.

Za učinkovito upravljanje in zaščito privilegiranih dostopov v organizaciji je treba zagotoviti:

- centralno upravljanje uporabniškega dostopa do nadzorovanih virov,
- preprečevanje nenadzorovane uporabe privilegiranih računov,
- zmanjšanje števila privilegiranih računov, potrebnih za upravljanje informacijskih sistemov,
- uporabo večfaktorske avtentikacije za dostop do privilegiranih računov,
- beležiti dostope z zapisi vseh poskusov uporabe privilegiranih računov,
- beleženje dejavnosti privilegiranega uporabnika,
- analizo zabeležene dejavnosti uporabnikov in preiskavo incidentov.

Axidian PAM

Rešitev Axidian PAM, ki jo podjetje OSI ponuja svojim naročnikom, izpolnjuje vse varnostne zahteve še tako zahtevnega naročnika. Hrani informacije o vseh privilegiranih računih in povezanih dovoljenjih za njihovo uporabo.

OSI d.o.o.
Ukmarjeva ulica 2, 1000 Ljubljana
info@osi.si
+386 (0)31 375 179
www.osi.si

Dovoljenja in politike

Dovoljenja se uporabljajo za določanje naslednjih parametrov dostopa:

- **kdo** – kateri uporabniki ali skupine uporabnikov imajo dostop;
- **kje** – s katerimi strežniki, strojno opremo in aplikacijami lahko delajo uporabniki;
- **pravice dostopa** – kateri račun bo uporabljen za povezavo;
- **kdaj** – obdobje dostopa in urnik, vrste protokolov, ki jih je treba uporabiti.

Dovoljenja centralno dodeli skrbnik v upravljalni konzoli Axidian. Če dostop ni več potreben, so dovoljenja lahko začasno onemogočena ali preklicana.

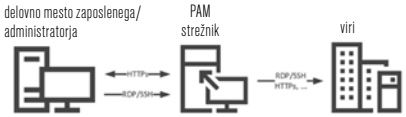
Politike se uporabljajo za definiranje splošnih parametrov dostopa in zajemajo načine dostopa do Windows, Linux/Unix sistemov, dovoljene in prepovedane ukaze v sejah SSH, (ne)zahtevane odobritve skrbnika PAM za odpiranje privilegiranih sej, lokalne vire osebnega računalnika, ki so na voljo na oddaljenem viru (diski, odložišče itd.), (ne)ponastavitev gesla privilegiranega računa po koncu seje, ekskluzivni način za privilegirane račune, kjer je en račun mogoče uporabiti samo za začetek ene seje, najdaljše trajanje privilegirane seje ter terminsko omejitev – kdaj lahko privilegiran uporabnik vzpostavi sejo na določen sistem.

Ključne prednosti Axidian PAM rešitve

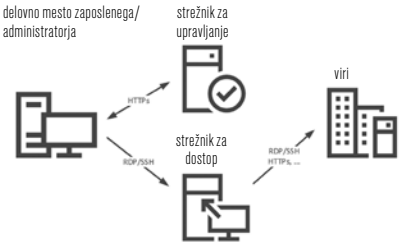
Rešitev Axidian PAM ponuja več načinov dostopa, in sicer RDP, SSH, http(S), Telnet, SFTP in SCP. Na končne strežnike se lahko prijavite z uporabniškim imenom in geslom (z možnostjo prikaza gesel, glede na pravice, ter njihovo menjavo) ali s SSH ključi. Axidian PAM upravlja z računi končnih sistemov, kot so Windows, Linux, AD in DBMS (MS SQL, PostgreSQL, MySQL, Oracle …) ter uporabniškim repozitorijem AD. Uporablja dvonivojsko avtentikacijo z uporabniškim imenom in geslom ter TOTP (t.i. *Time-based one-time password*). Aktivnosti se spremljajo v tekstovnih zapisih, v videih z možnostjo nastavljanja FPS in ločljivosti in zaslonskih slikah. Rešitev ponuja dva načina oddaljenega dostopa: MS RDS in SSH proxy.

Različni načini postavitve Axidian PAM rešitve

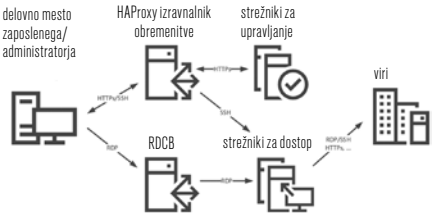
Osnovna: Management in Access servisa sta na istem strežniku



Razširjena: Management in Access servisa sta na ločenih strežnikih



Postavitev v HA (t.i. *High Availablity*)



Nakup in implementacija Axidian PAM rešitve

Podjetje OSI, kot avtorizirani partner podjetja Axidian za prodajo in implementacijo v Sloveniji, svojim naročnikom ponuja vseobsežne storitve vzpostavitve PAM rešitve. Za svoje naročnike izvajajo tudi namestitve in prilagajanje modulov ter integracije z njihovimi obstoječimi sistemi. Pripravijo vso potrebno sistemsko infrastrukturo za učinkovito uporabo PAM rešitve ter izvajajo izobraževanja, da lahko vsak naročnik implementirano rešitev uporablja samostojno – brez dodatnih skritih stroškov. (P.R.)

PODJETJE RESULT: AI REŠITVE PO MERI

Podatki: temelj za učinkovito implementacijo AI

Ključni koraki pri pripravi podatkov za uspeh v svetu umetne inteligence.

Stevanče Nikoloski

Vhod v areno umetne inteligence (AI) ne predstavlja zgolj obetavnih priložnosti, temveč postavlja nove zahteve po metodološki pripravljenosti podjetij. Uspeh v tej novi dobi ni odvisen samo od implementacije AI rešitev, temveč od globine razumevanja in priprave, ki je predhodnik k uvedbi teh tehnologij. Podatkovna priprava kot temeljna faza predstavlja kritično točko, ki precej določa uspeh ali neuspeh »umetno« inteligentnih sistemov.

Čiščenje in strukturiranje podatkov

Zakaj je priprava podatkov tako ključnega pomena? V jedru AI sistemov leži raznolikost in kompleksnost podatkov, katerih kvaliteta ima neposreden vpliv na robustnost in verodostojnost izhodnih rezultatov. Pravilno pripravljeni podatki tvorijo osnovo za natančne, zanesljive in učinkovite predikcije, ki so temelj vseh pametnih AI aplikacij.

Čiščenje podatkov je prvi esencialni korak, ki obsega detekcijo in odstranjevanje anomalij in napak v podatkovnem nizu. To ni le odpravljanje očitnih netočnosti, temveč tudi prepoznavanje in interpretacija manj zaznavnih vzorcev, ki lahko izkrivljajo analize. Vsak element, od nepopolnih zapisov do nekonsistentnih merilnih enot, zahteva pozornost, da se zagotovi čistost in zanesljivost podatkovnega sklopa.

Strukturiranje podatkov zahteva izbiro ustreznih metod za normalizacijo, segmentacijo in transformacijo podatkov v format, ki omogoča najučinkovitejšo obdelavo s strani AI. Oblikovanje strukturiranih podatkovnih nizov, ki omogočajo modelom, da zaznajo pomembne povezave in sklepajo smiselne vzorce, je ključno za nadaljnji proces učenja in napovedovanja.

Enako pomembno je tudi učinkovito shranjevanje podatkov

Priprava podatkov za učenje AI modelov je več kot le tehnična obveznost – gre za strateško odločitev, ki določa, kako bo sistem razumel in reagiral na raznovrstne podatkovne vire. Tehnike vzorčenja, razdelitev podatkov na učne in testne množice ter tehnike kodiranja za pretvorbo kategoričnih v številčne podatke so zgolj nekateri izmed korakov, ki zagotavljajo, da AI modeli delujejo optimalno in proizvajajo zanesljive rezultate.

Nenazadnje učinkovito shranjevanje podatkov postaja vse bolj ključno, saj obseg in raznolikost podatkov naraščata. Podatkovna jezera in skladišča morajo biti zasnovana tako, da omogočajo hiter in varovan dostop do podatkov, skupaj z zagotavljanjem integritete in varnosti informacij.

Celostna podpora podjetja Result

V podjetju Result razumemo, da je pot do uspešne implementacije AI tlakovana z dobro pripravljenimi podatki. Naša zavezanost k zagotavljanju visokokakovostnih, relevantnih in natančno obdelanih podatkovnih nizov je temelj, na katerem gradimo naše storitve. Ponujamo celostno podporo – od zbiranja in čiščenja do analize in interpretacije podatkov – da zagotovimo, da vaše poslovne odločitve temeljijo na trdnih, zanesljivih in inteligentnih podatkih.

Kakovostni podatki so tisti, ki dajejo smisel investiciji v AI – so valuta, s katero plačujemo za boljše, hitrejše in pametnejše odločitve. Z izrabo naših inovativnih pristopov in naprednih tehnoloških rešitev vam lahko pomagamo, da transformirate vašo množico podatkov v pravo podatkovno zlato.

Z nami se pripravite na prihodnost, kjer so »Use data. Live better!« več kot besede – so vaša nova realnost. (P.R.)

Avtor: Stevanče Nikoloski

SAFETICA

Preizkušene zmožnosti za uresničevanje zahtev NIS2

Direktiva NIS2 in prihajajoča nacionalna zakonodaja podjetja postavlja pred nove naložbe v kibernetsko varnost in upravljanje s tveganji.

Slovenska velika in srednja podjetja ter njihovi dobavitelji, ki po direktivi NIS2 spadajo med bistvene in pomembne subjekte, bodo morala že v letošnjem letu izvesti nove naložbe v zagotavljanje močnejše kibernetske varnosti. Zaradi obsežnosti ukrepov podjetja ne bodo mogla računati na rešitev vse v enem, temveč bodo prisiljena pridobiti več rešitev in storitev različnih ponudnikov glede na zahteve posameznega področja ukrepov v NIS2.
V podjetju Si splet so pripravili začetni pregled ukrepov, ki jih podpirajo s svojimi rešitvami in storitvami oziroma z rešitvami vodilnih evropskih proizvajalcev, kot sta ESET za kibernetsko varnost ter Safetica za preprečevanje odtekanja podatkov.

Analiziranje in upravljanje s tveganji

Z rešitvami Safetica ONE ter NXC lahko podjetja vseh velikosti hitro izvedejo revizijo podatkov in ugotovijo, katere vrste podatkov se uporabljajo v organizaciji, ne glede na to ali se nahajajo v lokalnem omrežju ali v oblaku. Poleg tega omogočajo pregledovanje informacijskih tokov in shranjevanje občutljivih podatkov, spremljanje dejavnosti uporabnikov v realnem času in ustvarjanje samodejnih poročil o obdelavi podatkov. Na osnovi poznavanja tveganosti posameznih virov podatkov podjetja lažje vzpostavijo in nastavijo ustrezne varnostne kontrole za svoj zunanji kibernetski prostor ter notranje omrežje in končne točke.

DISTRIBUCIJA:
SI SPLET d.o.o.
Ukmarjeva 4, Ljubljana
01 428 94 05

prodaja@sisplet.com
www.eset.com/si

Odzivanje na incidente

ESET zagotavlja zmožnosti in storitve za razširjeno odkrivanje in odzivanje na kibernetske grožnje (XDR, MDR), ki vključuje tudi proaktivno lovljenje groženj. Poleg tega nudi obveščanje o aktualnem stanju v kibernetskem prostoru, vpogled v vektorje napada, kibernetsko forenziko ter strokovne analize že potencialno škodljivih datotek. Storitev ESET MDR zagotavlja odzivanje na incidente že ob vzpostavitvi storitve. Ponuja vrsto ključnih funkcij in prednosti za izboljšanje kibernetske varnostne drže organizacij. Združuje umetno inteligenčno avtomatizacijo s človeškim strokovnim znanjem in obsežnim poznavanjem groženj, kar zgotavlja hitro odkrivanje groženj in odzivanje na incidente. Neprestan dostop do varnostne storitve, ki deluje v režimu 24/7/365, zagotavlja premostitev vrzeli v strokovnem znanju in razbremenjuje notranje varnostne ekipe.
Safetica v primeru kršitve varnosti podatkov preko sistema za opozarjanje v realnem času po elektronski pošti obvesti ustrezno osebje. Obvestilo zagotavlja vse podrobnosti, tako da lahko odzivne ekipe takoj izvedejo nadaljnje ukrepe in zmanjšajo posledice uhajanja podatkov.

Upravljanje varnostnih politik

Rešitve Safetica preprosto razvrstijo podatke, tako da so pripravljeni za izvajanje politike preprečevanja odtekanja podatkov. S tem podjetje vzpostavi tudi pravila uporabe in določi ustrezno obnašanje uporabnikov, ki dostopajo do občutljivih podatkov ali jih obdelujejo. Podobno tudi platforma ESET PROTECT zagotavlja implementacijo varnostnih politik in posledično avtomatizacijo varnostnih kontrol.

Obvladovanje ranljivosti

Platforma ESET PROTECT vključuje integrirano upravljanje ranljivosti in popravkov ESET Vulnerability and Patch Management. Gre za zmožnost, ki sledi nenehnemu razvoju groženj v kibernetskem okolju, vključno z napadi ničelnega dne, ter zagotavlja tekoče varnostno nadgrajevanje programske opreme informacijskih sistemov. Avtomatizirano pregledovanje in širok nabor možnosti filtriranja organizacijam omogočata hitro prepoznavanje in osredotočanje na varnostne težave, ki so zanje najpomembnejše. Poleg tega lahko podjetja z možnostmi samodejnega in ročnega popravljanja zagotovijo, da so njihove končne točke pravočasno posodobljene z najnovejšimi varnostnimi popravki.
V podjetju Si splet, ki deluje kot ESET Slovenija, so že lokalizirali tudi ESET-ove programe za usposabljanje in ozaveščanje o kibernetski varnosti, ki segajo od prilagojenih vsebin za otroke do certifikacijskih programov za zaposlene. Tako podjetjem omogočajo, da ob tehnični in organizacijski zaščiti usposobijo svoje zaposlene za varno nastopanje v kibernetskem prostoru, ne glede na to, ali delujejo v službenem ali domačem omrežju. (P.R.)

SYNOLOGY

Profesionalni video nadzor imate lahko tudi doma

Rešitev Surveillance Station Synology omogoča izgradnjo razširljivega nadzornega sistema, ki je primeren tako za domačo uporabo, kot tudi za velike namestitve, npr. za varovanje večjih parkirišč.

Ena od pomembnih možnosti, ki jih ponuja tajvanski proizvajalec strežnikov NAS Synology, je tudi vzpostavitev lastne nadzorne postaje. Svojo rešitev Surveillance Station razvija že več kot desetletje. Z več kot pol milijona aktivnih namestitev in več kot tremi milijoni upravljanih kamer si je Surveillance Station prislužila svoje mesto kot ena najbolj priljubljenih in zaupanja vrednih sistemov za video nadzor, tako med zasebnimi kot poslovnimi uporabniki.

Ljubljanska parkirišča nadzira Synologyjeva rešitev. Centralni sistem nadzora povezuje 296 kamer na več kot 30 parkiriščih na širšem območju Ljubljane. V ločen sistem za potrebe snemanja prometa in potopnih stebričkov pa je povezano še dodatnih približno 100 kamer. Študijo primera si oglejte na spletni strani podjetja Xenon forte d.o.o.

Omogoča spremljanje slike v visoki ločljivosti v živo iz več IP kamer, predvajanje posnetkov, urejanje nastavitev kamer, povezovanje z drugimi napravami in še veliko več. V podporo vse bolj zahtevnim implementacijam ima najnovejša različica Surveillance Station 9.0 preoblikovan uporabniški vmesnik, ki brezhibno združuje različne vire, kot so na primer kamere, zemljevidi, nadzor predvajanja in opozorila v eno nadzorno ploščo, ki nudi izboljšan pregled nadzorovanega prostora.

Nova različica podpira tudi dvojno snemanje in omogoča istočasno pretakanje nadzornih posnetkov v oblačno storitev C2 Surveillance, ki je posebej zasnovan za zmanjšanje potencialne izgube podatkov na le nekaj sekund. C2 Surveillance zagotavlja, da so posnetki vedno dostopni tudi po katastrofalnem dogodku ali v primeru kraje sistemov iz prostorov, ki jih varujejo. Domači uporabniki in podjetja so lahko brez skrbi in jim ni treba vlagati sredstev v drage in zapletene rešitve – popolna zaščita podatkov je res le en klik stran. Poleg tega pa je rešitev za uporabnike naprav Synology brezplačna.

IP kamere za vse vremenske razmere

Lani je Synology predstavil tudi svoji prvi dve kameri, ki sta zasnovani za brezhibno integracijo s Surveillance Stationom. Vso konfiguracijo kamer in omrežne nastavitve je mogoče upravljati neposredno v okolju, ki je nameščen na strežniku NAS ali NVR Synology. Poleg tega kamere Synology ne zahtevajo nakupa ali aktivacije licenc v rešitvi Surveillance Station, kar poenostavi postopek namestitve, omogoča enostavno selitev in zmanjša skupne stroške.

Kameri BC500 in TC500 sta opremljeni z zmogljivimi možnostmi umetne inteligence, ki uporabnikom zagotavljajo pravočasna in natančna opozorila, kar omogoča hitrejši odziv na dogodke. Funkcije, vključno z zaznavanjem ljudi in vozil, zaznavanjem motenja posesti in takojšnjim iskanjem, omogočajo uporabnikom, da bolj zanesljivo prepoznajo potencialne grožnje, hitro raziščejo izbrana področja ter hitro najdejo in pridobijo posnetke izbranih dogodkov.

Analitika, podprta s tehnologijo poglobljenega učenja

Za vse, ki bi želeli dodatne funkcionalnosti svojega nadzornega sistema, pa je na voljo naprava DVA. Prihaja v dveh različicah in omogoča dodatne funkcije, kot sta prepoznavanje obrazov in registrskih tablic vozil. Analitika globokega učenja lahko pomaga avtomatizirati upravljanje sistema, na primer z identifikacijo pooblaščenih oseb ali izračunom zasedenosti. In nenazadnje lahko pomaga tudi pri ustvarjanju statističnih podatkov in drugih koristnih informacij. DVA1622 podpira izhod HDMI za do 16 tokov na enem zaslonu in lokalno upravljanje z uporabo dveh vrat USB, kar odpravlja potrebo po uporabi osebnega računalnika za spremljanje in upravljanje nadzornega sistema.

Nadzor ne pomaga le ohranjati varnosti podjetij, ampak je v pomoč tudi pri učinkovitem upravljanju prostorov. Z DVA lahko avtomatizirate tudi prepoznavanje oseb, ki jim je prepovedan vstop na posest, zagotovite, da lahko samo pooblaščeni vstopajo v območja z omejenim dostopom ter ohranjate zasebna parkirišča prosta, brez skrbi, da bi jih kdo zasedel.

Synology nenehno razvija svojo rešitev in poenostavlja uvajanje, upravljanje in delovanje sistemov video nadzora. Njegova velika prednost pred konkurenco pa je, da ko enkrat postavite sistem nadzora, praktično nimate več dodatnih stroškov.

Več najdete tudi na spletni strani www.xenon-forte.si. (P.R.)

IBM GUARDIUM INSIGHTS SAAS DSPM

Zavarujte in prevzemite nadzor nad podatki v oblaku

Razvoj storitev v oblaku je odprl vrata novemu valu zapletenosti na področju podatkov.

Izzivi ne zajemajo samo identifikacije in sledenja različnim lokacijam hrambe podatkov, temveč tudi razumevanje njihove uporabe in dostopnosti, predvidevanje sprememb, ki jih prinese uvedba novih storitev, ter usklajevanje z raznolikimi predpisi, ki se med državami lahko razlikujejo.

Izziva se je pričakovano lotil IBM z naborom rešitev IBM Security, s katerim so postali globalni kibernetski ščit proti aktualnim grožnjam. IBM slovi po investicijah v raziskave in razvoj, ki redno prinašajo inovacije na področju varnostnih tehnologij. V prizadevanjih za nadgradnjo svoje varnostne ponudbe se opirajo na umetno inteligenco, strojno učenje in kvantno računalništvo.

IBM-ova umetna inteligenca Watson je na primer ključni element pri analiziranju velikih količin varnostnih podatkov za vpogled in samodejno odkrivanje groženj. IBM X-Force razkriva morebitne grožnje in ranljivosti, z rešitvami za upravljanje dostopa pa so našli odgovor na vprašanje upravljanja identitet. Končne točke, oblak, omrežje, neoporečnost podatkov — IBM se je lotil prav vseh najtežjih izzivov sodobnega kibernetskega okolja.

Enormni podvig pa zahteva strateška partnerstva. Skozi leta so se jim na poti pridružila številna podjetja. Red Hat, Trusteer in podobni so združili znanje v en ekosistem in s skupnimi močmi razvijali rešitve, ki danes skrbijo za varnost podjetij po vsem svetu.

Lansko leto se je ekosistemu IBM pridružilo še kibernetsko zagonsko podjetje Polar, ki je v nabor rešitev IBM Guardium dodalo sistem za upravljanje varnostne drže podatkov (angl. data security posture managament; DSPM), s katerim so se lahko lotili varnosti podatkov v oblaku.

Prevzemite nadzor nad podatki v oblaku in odkrijte vrzeli v podatkovni politiki

Do leta 2025 bodo po podatkih IBM-a vse nove aplikacije privzeto delovale na oblaku. Ta bliskovit prehod na oblačno infrastrukturo je predstavil nove organizacijske obremenitve za spremljanje ogrodij aplikacij, kar vključuje podatke, dovoljenja in drugo. IBM Guardium Insights SaaS DSPM, ki uporablja tehnologijo podjetja Polar, vam bo pomagal, da prevzamete nadzor nad podatki v oblaku.

Neustrezna organizacija je privedla do t. i. podatkov v senci (angl. shadow data), ki niso pod nadzorom IT ekip in povzročajo razdruževanje informacij. Zato je bil prevzem podjetja Polar ključen za IBM, kajti odtlej so lahko natančno ugotovili, kje so shranjeni ti občutljivi podatki v senci, za kaj se uporabljajo, hkrati pa so lahko opazili vrzeli v varnostnih politikah in varnostni drži podatkov.

IBM Guardium Insights SaaS DSPM vam pomaga odkriti poti, po katerih potujejo podatki v oblaku in storitvah SaaS. Za pravilno varnostno držo podatkov in izpolnjevanje skladnostnih zahtev je pomembno razumevanje in spremljanje tovrstnih podatkovnih tokov. Na novo vzpostavljen nadzor nad podatki v oblaku pa zagotavlja tudi možnost odpravljanja ranljivosti, posledično tudi hitrejši odziv za sprejem ukrepov za okrepitev varnostnih strategij, in izboljšanje upravljanja podatkovnih virov v oblaku.

IBM Guardium Insights SaaS DSPM – rešitev za pravilno varnostno držo podatkov

Kaj zajema pravilna varnostna drža podatkov? IBM Guardium Insights SaaS DSPM vam bo odkril podatke v senci, jih vrnil pod vaše okrilje in preprečil nepooblaščene dostope do občutljivih podatkov. Z nadzorom nad vsemi tokovi v oblaku boste lahko pozorno spremljali gibanje podatkov med okolji v oblaku, aplikacijami SaaS in tako preprečili uhajanje podatkov v napačne roke. Oblak je nedvomno prihodnost. Prej kot boste poskrbeli za varnost podatkov v oblaku, prej boste lahko začeli koristiti celoten potencial, ki ga ponuja. Več o tem, kako do pravilne varnostne drže podatkov, najdete na www.ibm.com. (P.R.)

OŽIVITE SVOJ DOGODEK

Digitalni LED pingvini: novi trend v vizualnih prikazih

Ponosno predstavljamo pametne digitalne LED pingvine - inovativne naprave, ki prinašajo novo dimenzijo vizualne komunikacije na vaše dogodke in prireditve.

Kaj sploh so digitalni LED pingvini?

Digitalni LED pingvini so inovativni LED zasloni, ki združujejo velikost tradicionalnih roll-up oglasnih panojev s sodobno tehnologijo.

Prednosti digitalnega LED pingvina v primerjavi s tradicionalnim roll-up pingvinom

Pri organizaciji dogodka ali prireditve se pogosto soočamo s pomembnim vprašanjem: kako pritegniti in zadržati pozornost občinstva? Tradicionalni roll-up oglasni panoji so sicer učinkoviti, vendar pa se v današnjem hitrem tempu življenja vse bolj nagibamo k dinamičnim in interaktivnim doživetjem. Točno tu pridejo v ospredje digitalni LED pingvini, ki ponujajo številne prednosti pred statičnimi grafikami.

Pametno upravljanje

Digitalni LED pingvini omogočajo široko paleto možnosti povezovanja in upravljanja, kar zagotavlja izjemno prilagodljivost glede na potrebe in želje uporabnikov. Uporabniki lahko vsebino naložijo na LED pingvine na več načinov. Hitri USB ključek je priročna možnost za prenos vsebine neposredno na napravo. S povezovanjem telefona ali računalnika preko WIFI modula na LED pingvinu je mogoče enostavno poslati željeno predstavitveno vsebino. Poleg tega je na voljo tudi možnost upravljanja preko namenske oblačne storitve, kar omogoča uporabnikom oddaljeni nadzor nad LED pingvini.

Robustnost in stabilnost

Z izjemno robustno konstrukcijo zagotavljajo stabilnost in vzdržljivost v različnih okoljih. Visokokakovostni materiali vam zagotavljajo njihovo dolgo življenjsko dobo in profesionalno uporabo, ne glede na prostor namestitve. Svojo stabilnost ohranjajo tudi med premikanjem na koleščkih, kar omogoča enostavno prenašanje in postavljanje na različne lokacije.

Notranja in zunanja uporaba

V osnovi so modeli zasnovani predvsem za notranjo uporabo, saj so v skladu z zaščito zaslona IP20, ki ga ščiti pred prašnimi delci. Njihova izjemna svetilnost, ki presega 1.000 nitov, zagotavlja več kot zadovoljivo uporabo in vidnost v vseh notranjih prostorih.

Za zunanjo uporabo so na voljo zunanji zasloni, ki ustrezajo zaščiti IP65, kar zagotavlja odpornost proti prahu in dežju ali snegu. S svetilnostjo 5.000 nitov omogočajo odlično vidnost v vseh pogojih, vključno z direktno sončno svetlobo.

Možnost združevanja

Z možnostjo enostavnega povezovanja več enot med seboj lahko ustvarite ogromne zaslone, ki izstopajo in privabljajo pozornost. Združevanje več LED pingvinov omogoča tudi izboljšanje ločljivosti za še bolj impresivno vizualno izkušnjo. Ta prilagodljivost vam omogoča, da svojo ustvarjalnost izrazite na najboljši možni način in zagotovite, da bodo vaša sporočila opazna in nepozabna.

Digitalne LED pingvine lahko najamete ali kupite glede na potrebe vašega dogodka ali poslovanja. Ne glede na to, ali potrebujete kratkoročno rešitev za poseben dogodek ali dolgoročno investicijo za stalno uporabo, vam v podjetju Strim plus nudijo prilagojene možnosti. Vse prednosti uporabe vam z veseljem pokažejo ob obisku njihove predstavitvene sobe z zasloni. Njihovi strokovnjaki vam svetujejo, da boste zagotovo izbrali optimalno rešitev za svoj posel. Več o digitalnih LED pingvinih si lahko preberete na spletni strani podjetja Strim plus: strim.si/digitalni-led-pingvini. (P.R.)

TECH TRADE D.O.O. TRZIN

UPS in prenapetostna zaščita: ključna v poslu, koristna tudi doma

UPS sistemi in prenapetostne zaščite zagotavljajo neprekinjeno napajanje in varujejo opremo pred poškodbami. Podjetje Tech Trade Trzin ponuja vrhunske rešitve za poslovno in domačo rabo.

Zanesljivost električne energije je ključnega pomena, a se tega pogosto zavemo šele takrat, ko ostanemo brez napajanja. Ste kdaj kaj ustvarjali na računalniku in je kar naenkrat zmanjkalo elektrike? Takrat ste izgubili tudi vse dokumente, ki jih niste shranili. Za to obstaja enostavna rešitev – UPS sistemi oziroma naprave za neprekinjeno napajanje, ki vas varujejo pred motnjami v električnem omrežju.

Nepogrešljivi pripomočki v ohranjanju stabilnosti elektronskih naprav so tudi prenapetostne zaščite, ki preprečujejo prehod previsoke napetosti v napravo, kar lahko povzroči trajno škodo ali celo uničenje opreme.

Tako UPS kot prenapetostne zaščite so nekaj, kar je v podjetju skoraj nujno, saj zagotavljajo neprekinjeno delo, stabilnost in zaščito naprav. V poslovnem svetu predvsem strežnikov, omrežne opreme, industrijskih kontrolnih sistemov … Podjetje Tech Trade Trzin, priznani dobavitelj elektronskih komponent, ponuja izdelke vrhunske kakovosti, med katerimi izstopajo rešitve priznanih blagovnih znamk, kot so Digitus, Mikrotik, Ubiquiti, Teltonika, Energenie.

UPS: zanesljiva zaščita pred napajalnimi prekinitvami

UPS sistemi so torej ključni za zagotavljanje nenehnega napajanja elektronskih naprav tudi v primeru izpada električne energije. Ponujajo neprekinjeno oskrbo z električno energijo, kar ne omogoča le nemotenega delovnega procesa, temveč tudi preprečuje poškodbe opreme.

Tech Trade Trzin ponuja širok izbor UPS sistemov, ki ustrezajo različnim potrebam in zahtevam uporabnikov. Blagovne znamke, kot so Digitus, Teltonika in Energenie slovijo po svoji zanesljivosti in visoki učinkovitosti. Pri njih najdete UPS sisteme za nekaj deset evrov, ki so lahko za manj zahtevne uporabnike povsem dovolj, da ob izpadu električne energije opravijo do konca, kar so želeli in na računalniku po nepotrebnem ne izgubijo podatkov, do UPS »rackov« za evrskega tisočaka ali več. Navadno vas te naprave ščitijo tudi pred prenapetostjo, kratkimi stiki in ostalimi nevarnostmi, ki pretijo računalnikom, strežnikom, omrežnim napravam in komunikacijskim sistemom.

Omislite si jih lahko v poslovnem ali domačem okolju. Doma služijo kot zaščita občutljive elektronike – televizorjev, igralnih konzol, pametnih domačih sistemov in osebnih računalnikov. Konec koncev so lahko zelo dobra izbira tudi za delo od doma, ko prav tako kot na delovnem mestu ne želimo izgubiti vsega, kar smo naredili v pretekli uri ali dveh.

Pred nakupom pa se je modro posvetovati s strokovnjaki, ki bodo dobro vedeli, kateri UPS bo najbolje opravljal to, kar boste od njega zahtevali.

Varovanje pred škodljivimi napetostnimi nihanji

Najmanj, kar si želimo je, da trenutek previsoke napetosti v električnem omrežju uniči napravo, kar se lahko zgodi, če ne poskrbimo za prenapetostno zaščito. Tako doma, še bolj pa v poslovnih okoljih, imamo preveč naprav, ki so ključne za poslovanje ali pa smo vanje vložili preveč sredstev, da bi jih zaradi svoje malomarnosti bili pripravljeni v trenutku izgubiti.

Prenapetostna zaščita je ključni del sistema za zaščito elektronskih naprav pred škodljivimi napetostnimi nihanji oziroma nenadnimi skoki in elektromagnetnimi motnjami. Te naprave delujejo tako, da preprečujejo prehod previsoke napetosti v električno napravo, vam pa prihrani sive lase zaradi težav, saj lahko v najslabšem primeru privedejo do uničenja opreme.

Podjetje Tech Trade Trzin ponuja vrhunske prenapetostne zaščite, med katerimi izstopajo izdelki priznanih blagovnih znamk, kot so Digitus, Mikrotik in Ubiquiti.

Ključni v poslovnem okolju, modro pa jih je imeti tudi doma

Če želite širok izbor vrhunskih izdelkov, ki ustrezajo različnim potrebam in zahtevam uporabnikov, ter strokovno svetovanje, odklikajte na spletno stran podjetja Tech Trade Trzin ali jih obiščite. Izdelki, ki jih imajo v svojem portfelju, zagotavljajo optimalno zaščito elektronskih naprav pred nepričakovanimi težavami z električno energijo. Več lahko najdete na www.techtrade.si. (P.R.)

TECHTRADE
www.techtrade.si

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

MARS COMMERCE

Kakšen monitor potrebujete za delo in kakšnega za igranje iger?

Velikokrat tekmujemo, kdo ima najboljši računalnik in pri tem primerjamo grafične kartice, procesorje, pogone, tipkovnice in miške.

Šele proti koncu pa se omeni monitor, čeprav gre za osnovno komponento, brez katere ne more funkcionirati nobena pisarna ali strežnik. Tudi domač gaming brlog je le bleda senca brez monitorja, ki lahko izkoristi potencial zverinskih grafičnih kartic, ki so nam danes na razpolago. Pisarna in gaming soba pa zahtevata dva zelo različna monitorja, kjer sicer najdemo nekaj skupnih imenovalcev, vseeno pa je pozornost usmerjena povsem drugam.

Kaj potrebujete za delo? In kaj potrebujete za igranje iger? In pa še najpomembnejše vprašanje, kje najti dobre monitorje?

Jasnost, odzivnost in natančnost – vse, kar potrebujete za delo

Ločljivost 1080p (1920 x 1080) je še vedno najbolj priljubljena za delo in tudi za igranje iger pri ne preveč zahtevnem ljubitelju iger. FullHD ali 1080p bo več kot zadoščala za večino pisarniških opravil, za bolj napredna opravila pa priporočamo višje ločljivosti in tudi povsem drugačne panele. Če boste gledali podrobne specifikacije, boste naleteli na izraze IPS, VA in TN, ki označujejo, katera panela je vgrajena v monitor. IPS monitor se lahko pohvali z dobro barvno natančnostjo, VA monitor pa se bolj osredotoča na kontraste. Če se ne ukvarjate s profesionalno fotografijo, je VA panela dobra in finančno bolj smiselna odločitev.

Kaj pa velikost? Najbolj priljubljeni diagonali sta 24 in 27 palcev. Večina uporabnikov združi dva ali celo več monitorjev, kar omogoča veliko boljšo produktivnost in razporeditev dela. Danes res težko najdemo pisarniško mizo brez dveh monitorjev. Na kaj morate biti še pozorni pri delu? Morda dobre vidne kote in pa vsaj osnovno zaščito pred modro svetlobo, saj vendarle 8 ur strmimo v pravokotno škatlo in vsaj na ta način prihranimo trpljenje našim očem.

Dahua monitorji, ki jih lahko najdete v podjetju Mars Commerce, izpolnjujejo vse naštete pogoje. Dahua C200 podpira ločljivost 1080p in 250 nit svetilnosti, kar zadošča za večino scenarijev, razen če boste monitor imeli postavljen neposredno na pot sončne svetlobe. Ima zelo dobre kontraste (3000 : 1) in pa tudi nekatere specifikacije, ki so pomembne za oblikovalsko delo: podpora za širok barvni razpon 99 % sRGB, 85 % NTSC in podobno. Ima tudi zaščito proti modri svetlobi in prilagodljivo frekvenco za preprečevanje trganja slike. Največja hitrost osveževanja je 75 Hz, kar zadošča za vse naloge z izjemo resnega igranja iger. Izbirate lahko med 24- in 27-palčnim modelom.

Dahua B200S je še en zanimiv pisarniški primerek. Ima zelo podobne specifikacije kot Dauha C200 in je prav tako na voljo z obema najbolj priljubljenima diagonalama. Ima pa kar 100-Hz hitrost osveževanja zaslona za še bolj gladko izkušnjo pri vsakdanjih nalogah. Podpira novejši HDMI in tudi starejši VGA priključek, ki je še vedno priljubljen v podjetjih. Podpira tudi namestitev na stojalo oziroma na steno. Tako lahko prihranite nekaj prostora na pisarniški mizi, morebiti pa tudi izboljšate ergonomijo delovnega prostora.

Gaming monitor mora zagotoviti občutek poglobljenosti

144 Hz je osnovna frekvenca, ki določa status vsakega gaming monitorja. Na drugem mestu je pomembna zakasnitev, na tretjem sta ločljivost in velikost, šele nato druge lastnosti. Dahua LM27-

E230C gre še korak dlje. Osvežuje se pri kar 165 Hz, odzivni čas pa je 5 milisekund. Na voljo je 27 palcev igralne površine, ki je obenem še ukrivljena (1500R), kar zagotavlja bolj poglobljeno izkušnjo med igranjem. Povezujemo pa se lahko preko najnovejših priključkov DisplayPort 1.2 in HDMI 1.4. Če boste želeli izkusiti najbolj grafično impresivne igre, kot na primer Cyberpunk 2077 ali Elden Ring, je to monitor, ki vam bo uspel pričarati tisto pravo gaming izkušnjo.

Po najboljše monitorje na …

… www.mars-commerce.si, kjer boste našli še več Dahua monitorjev in zagotovo boste našli enega ali dva, ki vam bosta olajšala delo ali pa popestrila zabavo med prostim časom. (P.R.)

TERATEC D.O.O.

Vrhunska varnost s kamerami, senzorji, kontrolo pristopa …

Izbira partnerja za tehnično varovanje doma ali poslovnega objekta je ključnega pomena. Izkušnje, znanje in predanost kakovosti so zagotovo faktorji, na katere morate biti pozorni.

Zaman je ponavljati in poudarjati pomen varnosti, če najprej ne poskrbite za svojo varnost in premoženje. Morda je zdaj pravi čas, da za to tudi nekaj naredite. Tehnično varovanje objekta, kot ga nudi podjetje TERATEC, je zagotovo korak v pravo smer.

Videonadzor za neprestano spremljanje

Eden izmed ključnih elementov tehničnega varovanja je videonadzor. Če lahko kjerkoli in kadarkoli preverite, kaj se v objektu ali okoli njega dogaja, bo to zagotovo pripomoglo k vaši varnosti in mirnosti. Nadzor s kamerami omogoča celovit vpogled v dogajanje na različnih lokacijah. To je izjemno koristno, še posebej v večjih objektih, kjer je potreben nadzor večjega območja. Zmožnost natančnega spremljanja dogodkov, kot so nepooblaščeni vstopi, požari ali morebitne nesreče, omogoča hitro in učinkovito ukrepanje. Posnetki, pridobljeni s kamere, so tudi dragocen vir informacij v primeru morebitne policijske preiskave ali analize dogodka.

Senzorji za zaznavanje vloma

Še eno pomembno področje specializacije podjetja TERATEC predstavljajo protivlomni sistemi. S sistemi in senzorji za zaznavanje vloma omogočajo hitro in učinkovito reakcijo v primeru nepooblaščenega vstopa v objekt. Hitro obveščanje lastnika ali varnostne službe omogoča preprečevanje škode ali kraje premoženja.

Požar? Ukrepajte hitro

Poleg video nadzora in protivlomnih sistemov pa podjetje TERATEC ponuja tudi vrhunske sisteme za avtomatsko javljanje požara. Ob tovrstnih nepredvidenih dogodkih je hitro ukrepanje odločilno – z omenjenimi sistemi pa tudi zagotovljeno. Detektorji in požarne centrale omogočajo hitro in natančno lociranje nevarnosti in zmanjšujejo tveganje za večjo škodo.

Kdo ima dovoljenje za vstop na določeno območje?

Dotaknimo se še kontrole pristopa, ki jo ponuja podjetje TERATEC. S sistemom za nadzor pristopa lahko lastniki objektov natančno določijo, kdo ima dovoljenje za vstop v določene prostore ali območja. To je izjemno pomembno za omejevanje dostopa do občutljivih območij in zagotavljanje varnosti zaposlenih in obiskovalcev.

Obsežno znanje in izkušnje

Danes je varnost vedno večji izziv. Izbira partnerja za tehnično varovanje je zato zelo pomembna –

pri tem štejejo izkušnje, znanje in predanost kakovosti. podjetje TERATEC se osredotoča na zagotavljanje varnosti objektov in ljudi v njih. Njihove varnostne rešitve temeljijo na izkušnjah, pridobljenih v največjih slovenskih in tujih podjetjih za zasebno varovanje. Njihovi strokovnjaki ne zagotavljajo le brezhibne izvedbe tehničnega varovanja, ampak tudi svetovanje, kar zagotavlja optimalno in zanesljivo zaščito.

V podjetju Teratec Vam torej ponujajo storitev od začetka do konca, od ideje do vzdrževanja vgrajenega sistema.

Podjetje TERATEC se zavezuje k zagotavljanju najvišjih standardov kakovosti vgrajenih materialov in zanesljivosti svojih storitev. Podjetje TERATEC ponuja kompleksnost varnostnih potreb, ne glede na velikost objekta in celovite rešitve, ki jamčijo za vašo varnost v vsakem trenutku.

Več o njihovih rešitvah lahko najdete na spletni strani www.teratec.si. (P.R.)

MEGA M

Rešitev mCloud uporablja vse več poslovnih uporabnikov

Podjetje Mega M d.o.o. ponosno predstavlja svojo uveljavljeno rešitev v svetu IT storitev - mCloud.

Gre za celovito rešitev računalništva v oblaku, ki prinaša občutno optimizacijo IT infrastrukture, nižje stroške poslovanja ter omogoča popolno prilagodljivost in varnost.
Namesto nakupa fizičnih strežnikov se podjetja raje odločijo, da IT storitve prevzame nekdo, ki je za to usposobljen. Zakupijo se potrebne kapacitete, ki se dejansko uporabljajo, tekom poslovanja pa dodajajo ali odvzemajo, odvisno od potreb.

Podjetje Mega M z blagovno znamko MegaTel že 22 let na trgu telekomunikacij poslovnim in zasebnim uporabnikom zagotavlja širok nabor digitalnih in trajnostno usmerjenih storitev, tehnično podporo, enostavnost in prijaznost ter najpomembnejše – zadovoljstvo. Kot prvi operater v Sloveniji pa se lahko pohvali s kombinacijo petih storitev (»PETORČEK«): mobilna telefonija, IP telefonija, televizija, širokopasovne storitve ter rešitve na področju eMobilnosti.

Odlična infrastruktura v oblaku

mCloud zagotavlja virtualne strežnike z neomejeno podporo v delovnem času, hitro odzivnostjo in rednimi mesečnimi poročili o stanju. Storitev teče v lastnih lokacijsko ločenih podatkovnih centrih, kar zagotavlja redundanco in skladnost z vsemi slovenskimi ter EU regulativami o varovanju podatkov. S tem se podjetjem omogoča, da stopijo v korak s časom ter dosežejo občutno nižje IT stroške.

Prilagojene rešitve po meri

mCloud ne ponuja zgolj generičnih rešitev, ampak prilagaja svojo storitev posameznim potrebam uporabnikov. Gostovanje posameznih aplikacij, migracije baz aplikacij, gostovanje in zakup domen ter spletnih strani – vse to je mogoče prilagoditi glede na specifične zahteve stranke. S tem podjetjem omogoča fleksibilnost in optimalno delovanje v oblaku.

Vsestransko gostovanje

Podjetja lahko najamejo gostovanje spletnih strani ter poštnih predalov. Ponujajo osnovne in napredne poštne predale z vključenim varnostnim kopiranjem, kar povečuje varnost in zanesljivost poslovnih komunikacij.

Najnovejše Microsoft 365 rešitve

mCloud integrira vse Microsoft 365 rešitve v celovito storitev. To pomeni, da podjetja dobijo najnovejše orodje za produktivnost in sodelovanje, vse znotraj enotnega okolja.

Varna hramba podatkov

Storitev omogoča varno hrambo podatkov na tretjo lokacijo z uporabo Veeam rešitev za varnostno kopiranje po vnaprej določeni politiki. To povečuje varnost in zanesljivost shranjenih informacij.
Z mCloud storitvijo lahko podjetja opravljajo delo kjerkoli in kadarkoli, občutijo nižje IT stroške, zagotovijo 100 % zaščito pred izgubo podatkov ter ostanejo v skladu z zakoni in regulativami o varovanju podatkov (ISO 27001). mCloud predstavlja napredno rešitev, ki bo premaknila poslovanje v digitalno dobo.

Svetovanje in priprava ponudbe za najbolj optimalno virtualno pisarno:
prodaja@megatel.si ali preko 03 777 00 00. (P.R.)

Mega M d.o.o.
Rudarska cesta 6, 3320 Velenje
+386 3 777 00 40

info@megatel.si
www.megatel.si

KONFERENCA TOGETHER IN EXCELLENCE

Kako je AI spremenila poslovni svet

Nenadni vzpon in vse večja vloga umetne inteligence v poslovnem svetu sta postavila pred strokovnjake in praktike s področja projektnega vodenja ter upravljanja storitev IT tako nove izzive kot tudi nepredstavljive priložnosti.

Razvoj umetne inteligence (AI) je predrugačil način, kako organizacije izvajajo svoje dejavnosti, in prinesel pomembne spremembe v dinamiko dela ter odločanja.

V tem kontekstu se bliža konferenca TOGETHER IN EXCELLENCE – SKUPAJ DO ODLIČNOSTI 2024, ki bo potekala 15. maja v Ljubljani in bo združila izkušene strokovnjake in praktike obeh področij. Med predavatelji bodo tudi priznani evropski in ameriški strokovnjaki, ki bodo delili svoje dragocene vpoglede in izkušnje s področja umetne inteligence, projektnega vodenja in upravljanja storitev IT.

»Gre za dogodek, kjer se predstavljajo najnovejše in najboljše prakse, metodologije ter tehnologije,« pravi Mateja Čampa iz Združenja itSMF Slovenija, ki konferenco letos pripravlja že šestič. »Raznolike teme, ki jih pokrivajo letošnji govorci, od vloge umetne inteligence v IT storitvah do etičnih vidikov uporabe AI, od projektnih pisarn do minimalizma v projektih, ponujajo širok spekter vpogledov in strategij, ki lahko obogatijo naše pristope k projektnemu vodenju in upravljanju storitev IT.«

Prisluhnite najuglednejšim strokovnjakom

Med govorci bo konferenca gostila enega izmed najuglednejših strokovnjakov na področju projektne pisarne (PMO) in upravljanja projektov, America Pinta. Kot izkušen vodilni direktor pri PMO Global Alliance (PMOGA), Pinto predstavlja vodilno avtoriteto na tem področju. Predstavil bo svoje vpoglede in izkušnje, razpravljal o vlogi umetne inteligence pri projektih in upravljanju storitev IT ter pomenu prilagajanja PMO-jev prihodnjim zahtevam poslovnega okolja. »Pintovo predavanje je namenjeno strokovnjakom PMO-jev, vodjem in vsem, ki jih zanima strateška usmeritev projektne pisarne,« poudari Marko Golob, predsednik združenja za projektno vodenje, PMI Slovenija in ob tem doda: » Veseli nas, da na slovenski oder prihaja tudi Lee R. Lambert, vodilna osebnost, ki je prispevala k razvoju metodologij in praks vodenja projektov pri Project Management Institute. Govoril bo o vlogi umetne inteligence v projektnem vodenju in podal praktične nasvete za uspešno izvajanje projektov v dobi digitalne preobrazbe.« Ob upoštevanju hitrega napredka tehnologije in njenega vpliva na delovno okolje bo Lambert podal svoj pogled na to, kako lahko AI izboljša učinkovitost, produktivnost in kakovost v procesih projektnega vodenja. Med govorci se bo zvrstil tudi strokovnjak za projektno vodenje Nader K. Rad, ki bo obravnaval koncept minimalizma v projektivnem vodenju – kaj minimalizem je, zakaj deluje in kako lahko pristop minimalizma uporabimo v reševanju zapletenosti projektov.

Ob uporabi umetne inteligence se postavljajo pomembna vprašanja o etiki in varnosti. Kako zagotoviti, da UI deluje v skladu z etičnimi načeli in ne ogroža varnosti podatkov? Stephen Alstrup, priznani profesor, eden od vodilnih svetovnih strokovnjakov na področju algoritmov ter svetovalec danske vlade za digitalizacijo in varstvo podatkov, bo v svojem predavanju osvetlil pomembnost etike pri uporabi generativne umetne inteligence (GenAI). Poudaril bo potrebo po varnosti in skladnosti pri uporabi tehnologije, kje lahko GenAI prinaša resnično vrednost, pa tudi kje so njeni izzivi in morebitna tveganja. Podal bo praktične smernice in primere, ki bodo osvetlili vpliv GenAI na različne vidike poslovanja in družbe.

Udeleženci konference bodo lahko spoznali tudi različne načine, kako lahko AI spremeni operativni model IT in dobili vpogled v konkretne možnosti uporabe tehnologije v procesih upravljanja storitev IT. Rob Akershoek, vodilni arhitekt za upravljanje IT ter predsednik IT4IT Foruma v okviru organizacije The Open Group bo poudaril uporabo AI v razvoju in testiranju IT storitev, upravljanju varnosti, tveganj in skladnosti, napovedovanju izpadov storitev, avtomatizaciji operacij ter še mnogo več. Akershoek bo obravnaval tudi vprašanja, kako AI prispeva k ustvarjanju naslednje generacije ITSM, kakšni so koristi uporabe AI v ITSM ter kako tehnologijo integrirati v obstoječo IT infrastrukturo.

Skupno znanje, ki ga bodo občinstvu prinesli ti strokovnjaki, lahko pomaga pri razvoju inovativnih, učinkovitih in odgovornih pristopov k projektnemu vodenju in upravljanju storitev IT. Spremembe in izboljšave, ki temu sledijo, so ključne za uspeh organizacij v poslovnem okolju. Za več informacij o dogodku in registracijo obiščite spletno stran konference. (P.R.)

info@togetherinexcellence.si
www.togetherinexcellence.si

Posebna ponudba za dijake, študente in upokojence!

V reviji najdete članke o:

biologiji

astronomiji

računalništvu

avtomobilizmu

ter o mnogih drugih tehnoloških in naravoslovnih tematikah!

Ob sklenitvi naročnine knjižno darilo!

Naročam se na revijo *Življenje in tehnika*:

- ○ Letna naročnina **55€**
- ○ Letna naročnina za dijake, študente in upokojence **49€**

Kopijo kartice upokojenca oz. potrdila o vpisu pošljite na mojca.borko@tzs.si ali po pošti na naš naslov.

Izberite knjižno darilo:

- ○ Digitalni zrcalno-refleksni fotoaparat
- ○ Skrivnosti inovacij Steva Jobsa
- ○ iZnanost
- ○ Ujemite trenutek

Poštnina plačana po pogodbi št. 88/1/S. Znamka ni potrebna.

*Ime in priimek:

*Ulica in hišna številka:

*Poštna številka in kraj:

*Telefon:

E-pošta:

*Podpis:

Tehniška založba Slovenije
Lepi pot 6
(p. p. 541)
SI - 1000 Ljubljana

Tehniška založba Slovenije | www.tzs.si narocila@tzs.si | MODRA ŠTEVILKA 080 17 90

Kako prepoznati spletne goljufije?

Katera iznajdba je bila najpomembnejša? Kolo, internet, morda umetna inteligenca? Argumenti za internet so močni: neskončen vir informacij, steber, ki drži pokonci sodobno družbo, orodje za poenostavljenje vsakdanjika …

Uporabljamo ga praktično za vse. Prek njega dostopamo do e-poštnih sporočil, iščemo novice, beremo knjige in stripe, igramo igre, nakupujemo, gledamo filme, serije, kratke posnetke – seznam se vije v neskončnost. Vsaka dobra stvar pa ima tudi svojo negativno plat. V tem primeru ima internet ogromen potencial za širjenje goljufij in lažnih informacij.

Če ste reden obiskovalec spleta, ni za lase privlečeno, da vsaj enkrat dnevno naletite na goljufijo (angl. scam) ali pa vsebino, ki se zdi na prvi pogled zelo sumljiva. Nekatere so zelo očitne, druge malenkost bolj prefinjene, pri tretjih pa je skoraj nemogoče prepoznati, da gre za kompleksno prevaro. Zadnji sklop postaja vse bolj pogost, za kar se lahko zahvalimo tudi umetni inteligenci, ki je pred dobrim letom postala splošno dostopna vsakemu uporabniku.

Če ste pravočasno prepoznali goljufijo, odlično. Vendar se v praksi dogaja ravno obratno – preveč ljudi kljub vsem opozorilom in akcijam ozaveščenosti o kibernetski varnosti še vedno prepozno ugotovi, da so tarča nepridipravov.

Kako prepoznati lažno spletno stran?

Ustvariti osnovno spletno stran je enostavno, registracija domene je opravljena v nekaj klikih in le za nekaj »centov«, v zameno pa nepridipravi dobijo zelo dobro osnovo, s katero lahko začnejo prežati na neprevidne in naivne uporabnike. Ker je postopek vzpostavitve spletne strani tako enostaven, je internet postal leglo lažnih spletnih strani. ChatGPT in podobni »boti« so samo še pospešili njihovo širjenje, obenem pa je lažne spletne strani vse težje prepoznati.

Nanje lahko naletimo z iskanjem določenega izdelka, lahko obskurnega ali trenutno najbolj vročega, pa prek oglasov, ki se lahko predvajajo tudi na verodostojnih platformah, kot je na primer Facebook. Prevečkrat sem dobil klic znanca, ki je preko Facebook objave prišel do super spletne strani, kjer lahko kupi komplet orodja

priznane blagovne znamke za le nekaj deset evrov (namesto nekaj sto evrov). Tam se znajdejo tudi PlayStation 5 po polovični ceni, morda grafična kartica RTX 4090, ki se običajno prodaja za 2000 €, a samo v tistem trenutku jo lahko dobite za ugodnih 800 €. Seveda se čas odšteva, ker je ponudba časovna omejena.

Velja pravilo: »Če kaj izgleda predobro, da bi bilo res, potem takšno ponavadi tudi je.« Če naletite na spletno stran s sumljivo ugodnimi ponudbami, bodite pozorni. Začnite raziskovati. Preberite ocene izdelkov, če obstajajo, in ignorirajte tiste generične komentarje, kot na primer »odličen izdelek«, »naprava je točno takšna, kot v opisu in še hitra dostava« in podobne.

Če spletne strani ne poznate oziroma na njej kupujete prvič, lahko njeno ozadje preverite na Googlu. Za začetek pojdite na slovenske forume in se pozanimajte, ali je kdo tam že kupoval/naročal storitve. Če je trgovina tuja, boste imeli več uspeha, če boste na koncu iskalnega niza dodali na primer »jetaspletnastrannateg. com scam reddit«. Na Redditu boste našli ogromno podskupin, ki se ukvarjajo s spletnimi goljufijami in morda boste našli pogovor ravno o vaši spletni strani.

Preverite lahko tudi ozadje spletne strani na whois.com. Preverite domeno, koliko časa je spletna stran registrirana … Kratek čas ni nujno pokazatelj goljufije, vseeno pa je lahko opozorilo, da raziščete globlje. Na domnevno lažni spletni strani poiščite kontakte prodajalca oziroma podjetja. Kaj se zgodi, ko pokličite na številk-

ko? »Pogooglajte« tudi fizični naslov in preverite, da Janez Novak d.o.o., ki prodaja elektroniko, ne obratuje v neki majhni slaščičarni.

Tudi načini plačila so lahko dober pokazatelj. Če jim ne zaupate, poskusite izbrati način plačila po povzetju. Imeli boste nekaj evrov več stroškov, a boste vsaj pomirjeni, ko bo paket dejansko prišel do vaših rok oziroma ne boste vnaprej plačevali za nekaj, česar nikoli ne boste prejeli.

Goljufi vas bodo želeli pretentati tudi z izjavami domnevno kredibilnih oseb. Mi smo naleteli na primer Petra Poljanška, podjetnika iz Ljubljane, ki so ga uporabili za promoviranje kačjega olja, spet drug dan je bil na drugi spletni strokovnjak za programsko opremo, SEO ali kaj drugega. Uporabili so sliko, ki jo lahko najdemo na internetu, in najverjetneje izmišljeno izjavo. Vsako sliko lahko preverite tako, da jo najdete s pomočjo Googlove funkcije Slikovno iskanje. Ogledate si lahko, kje vse na Googlu je že bila uporabljena. Lahko gre za »stock« fotografijo, vseeno pa spletna stran izgubi kredibilnost, če navaja lažne podatke.

Prevarajo vas lahko tudi na Amazonu, eBayu, Bolhi …

Naj vas ne zaslepi ime platforme, na kateri kupujete. Njihova verodostojnost še ne pomeni, da so vse ponudbe enako kredibilne. Amazon je sploh v zadnjih nekaj mesecih postal gnezdo tretjih prodajalcev, običajno kitajskih, ki prodajajo sanje. Lahko se zgodi, da boste pod ocenami našli super izkušnje, vendar se splača preveriti, ali je ta ocena pravzaprav sploh zares namenjena izdelku, ki ga kupujete. Amazon ima težave s prodajalci, ki legitimne izdelke zamenjajo z lažnimi, vendar pustijo enake ocene. Najboljše je, da kupujete izdelke, ki jih neposredno dostavlja Amazon (angl. fullfiled by Amazon) ali pa prodajalec, ki mu zaupate.

eBay je že od nekdaj znan po tem, da ima kopico lažnih prodajalcev, ki v droben tisk na primer napišejo, da prodajajo samo prazno embalažo ali pa celo samo fotografijo izdelka, seveda za maloprodajno ceno pravega izdelka.

Tudi na Bolhi smo že naleteli na lažne oglase, tudi pri tistih z oznako Brez skrbi. Ko boste želeli opraviti nakup, boste prejeli povezavo ali SMS sporočilo, ki vas bosta napeljevala na dokončanje nakupa na tretji strani (ki bo posnemala izgled Bolhe) ali pa izpolnitev določenih občutljivih podatkov. Upamo, da ni treba posebej poudariti, da v nobenem primeru ne delite svojih osebnih podatkov, kaj šele finančnih.

Kako prepoznati lažna sporočila?

Phishing sporočila (ribarjenje) so še vedno najbolj priljubljeno orodje v portfelju nepridipravov. In ta postajajo vse bolj prefinjena, kar pomeni, da jih bo z vsakim letom težje prepoznati. Včasih vam pošljejo phishing sporočilo ravno ob pravem trenutku. Ko je sodelavec testiral novo mobilno aplikacijo ene od slovenskih bank, je ravno dobil SMS sporočilo, da so mu zaradi sumljive aktivnosti zablokirali račun. Seveda je bila priložena povezava, kjer bi moral vpisati svoje podatke in tako overiti svojo identiteto. Povezava mu je bila takoj sumljiva, a verjamemo, da bi marsikdo v njegovi koži panično kliknil na povezavo.

Podobno smo v zadnjih mesecih dobili več sporočil o neuspešni dostavi pošiljke. Pošiljatelj je na prvi pogled Pošta Slovenije, v ozadju pa potrpežljiv nepridiprav. Če tako kot mi vedno pričakujete kakšno pošiljko, vas lahko takšno sporočilo ob pravem trenutku hitro zmede.

Tisti najbolj napredni uporabniki vsako sumljivo povezavo, datoteko … najprej odprejo v virtualnem okolju, kjer se lahko prepričajo o njeni kredibilnosti. Povprečen uporabnik spleta tega ne bo počel. Obstajajo pa tudi drugi znaki za lažna sporočila. Sumljiva povezava je prva, potem so še kakšne slovnične napake, slabi prevodi, nenavadni sestavki, tuja številka in nenavadno ime pošiljatelja. Če dobite občutek lažnosti, mu zaupajte. Nič vas ne stane, da na primer pokličete na banko ali pošto in se pozanimate, kaj se dogaja.

Najboljši nasveti za izogib goljufijam

- Redno spremljajte transakcije.
- Če boste prejeli sumljivo Facebook sporočilo, tudi če je pošiljatelj vaš prijatelj, ga ne odpirajte in neposredno kontaktirajte osebo.
- Če je le možno, pri spletnih nakupih uporabite virtualno kartico za enkratno uporabo, kot jo na primer omogoča Revolut.
- Na www.haveibeenpwned.com lahko preverite, ali je kateri izmed vaših poštnih naslovov ogrožen.
- In še enkrat poudarimo: »Če kaj izgleda predobro, da bi bilo res, potem takšno ponavadi tudi je.«

Dragon Ball FighterZ

Dragon Ball ostaja eden najbolj priljubljenih animejev (japonskih risank) vseh časov, FighterZ pa ena njegovih najboljših priredb. Gre za borilno igro v slogu Street Fighterja, le da je veliko bolj dostopna in spektakularna, kot je za to zvrst običajno. Izberemo si tri borce, ki bodo tvorili našo ekipo; seveda jih ne manjka in med njimi so ikonični, kot so Goku (v oblikah Super Saiyan in SSGSS), Piccolo in Vegeta (prav tako Super Saiyan in SSGSS). Med tepežkanjem hitro ugotovimo, da je nadzorna shema preprostejša kot navadno – uporabljamo le štiri gumbe za napad in ni zapletenih kombinacij smeri in gumbov kot v Street Fighterju. Namesto nanj so se ustvarjalci Dragon Ball FighterZ naslonili na drugi stripovski borilni naslov, Marvel vs. Capcom, saj poleg značilne nadzorne sheme kličemo na pomoč druge like iz ekipe in izvajamo napade ter kombinacije s celotnim moštvom. Igre se tako hitro naučiš, nudi pa veliko globine in dolgoročnega udejstvovanja tako s prijatelji za enim zaslonom kot po internetu. Slednje je poglavitna značilnost na novo izdanih inačic za PlayStation 5 in Xbox Series X/S, ki nadgradita prejšnji za PS4 in Xbox One. Ti verziji namreč vsebujeta naprednejšo, rollback spletno programsko kodo za bolj gladke internetne spopade.

MX vs ATV Legends – 2024 Monster Energy Supercross Edition

Dirkanje po blatnih, peščenih in skalnatih progah je za marsikoga preveč nevarno, da bi se ga lotil v resničnem življenju. Zato pa so tu videoigre, konkretno serija MX vs ATV, ki se iz dela v del izboljšuje. Najnovejša različica je MX vs ATV Legends, ki nas postavi v tri vrste vozil: na sedež motociklov in pa dveh vrst štirikolesnikov, manjših ATV-jev in večjih UTV-jev (to so tisti z varnostnim okvirjem nad kabino). ATV pomeni All-Terain Vehicle, UTV pa Utility Task Vehicle; z obema se vozimo čez drn in strn, le da so ATV-ji gibčnejši in boljši v ovinkih, UTV-ji pa masivnejši in varnejši. Kariera v igri nas posadi v vse tri vrste vozil in od nas terja mojstrstvo tako na odprtih progah z veliko ravnicami kot na ovinkastih stezah z množico skokov. Nadzor ni tako realističen kot v sorodni seriji Monster Energy Supercross, je pa zato bolj dostopen in neposredno zabaven. Grafika pa je na PlayStationu 5 zelo dobra, s podrobnimi teksturami in učinki škropljenja blata vsepovsod. No, igro so zdaj nadgradili z novo edicijo, ki vsebuje predvsem šestnajst uradnih prog iz prvenstva Monster Energy AMA Supercross, od Anaheima do Salt Lake Cityja. Ni boljšega za ljubitelje tega ameriškega tekmovanja!

Contra: Operation Galuga

Contra je stara in spoštovana serija od strani gledanih arkadnih strelskih iger, s katero smo se zabavali že v osemdesetih letih prejšnjega stoletja. V Evropi je morda nekoliko manj znana, med drugim zato, ker je za Super Nintendo tod izšla pod imenom Super Probotector. A to ne zmanjšuje njene odmevnosti in kakovosti. Vedno je šlo za napete in zahtevne streljanke, v katerih so te, če zadev nisi imel naštudiranih, pokončali v nekaj sekundah. Najnovejša epizoda se imenuje Operation Galuga in na prvi pogled gre za precej drugačno igro, saj je grafika preskočila v tri razsežnosti in je postala nekoliko bolj barvita. Toda igralno srce je ostalo enako. Pogled je še vedno tisti od strani, in še zmerom nadzorujemo enega od dveh vojačkov (Billa Rizerja ali Lancea Beana), ki se na Novi Zelandiji spopadeta s silami teroristične skupine Red Falcon. Tu so mogočna orožja, od laserja do vodenih raket, ki jih je mogoče tudi nadgrajevati in ki včasih v nekaj sekundah očistijo ves zaslon, da na njem ne ostane niti en sovražnik več … posebne veščine za vsakega od dveh komandosov … in ogromni šefi, ki se jim je treba kar konkretno posvetiti, sicer oni posvetijo nam. In nič bati, na razpolago so tudi nižje težavnosti!

TMNT Arcade: Wrath of the Mutants

Nindža želvaki so spet v modi, tudi na področju videoiger. Ker se je odlični Shredder's Revenge s še boljšim dodatkom Dimension Shellshock prodajal dobro in ker je šla za med tudi zbirka starejših želvaških naslovov Cowabunga Collection, smo zdaj dobili še TMNT Arcade: Wrath of the Mutants. Beseda »Arcade« daje vedeti, da gre za igro, ki so jo najprej naredili za igralne avtomate, in res je izvirnik v tej obliki luč sveta ugledal že pred sedmimi leti. Za nameček je stroj temeljil na Nickelodeonovi animirani seriji iz 2012, ki je razdelila občinstvo s samosvojim 3D »računalniškim« videzom. Skratka, vnovič gre za igro vrste »beat 'em up«, torej za pretepaško igro, v kateri hodimo proti desni in obračunavamo z množico sovražnikov. Igramo lahko sami ali v družbi drugih želvakov ter nasprotnike odstranjujemo s kombinacijami udarcev in mogočnimi specialkami, pomerimo pa se tako z običajnimi sitnobami kot s šefi. V novi izdaji igre je kar šest novih poglavarjev, avtorji pa so ustvarili še tri sveže stopnje in v snemalni studio znova povabili igralce, ki so posodili glas likom v seriji. Seth Green, Sean Astin, Rob Paulsen in Greg Cipes so tako posneli nove dialoge, kar bo zagotovo razveselilo vse ljubitelje nabritih kornjač.

InfoHiša AKADEMIJA Finance

10. DNEVI PRAVA ZASEBNOSTI IN VAROVANJA INFORMACIJ

18.–19. aprila 2024, Grand hotel Primus, Ptuj

IZ VSEBINE:

Uvodno predavanje: **Če bi bil David Attenborough DPO: Raziskovanje poti posameznika, na katerega se nanašajo osebni podatki**

Rie Aleksandra Walle,
ustanoviteljica NoTies Consultinga, DPO Huba in gostiteljica podkasta Grumpy GDPR

Govornica bo predstavila načine, kako se izogniti nepredvidljivim pastem in graditi zaupanje s posamezniki, ki postajajo vse bolj ozaveščeni na področju zasebnosti. Z vidika posameznika in njegovih pravic bo zajela izkušnje pri spoprijemanju z izzivi zasebnosti na mednarodnem področju, pri čemer bo poudarek na varnosti, piškotkih, prijavi na novičnike in politiki zasebnosti.

Na konferenci bomo pogledali, kakšno je bilo **prvo leto izkušenj Informacijskega pooblaščenca z ZVOP-2**, izkušnje in izzive upravljanja skladnosti po ZVOP-2 bodo delili tudi predstavniki **Fursa, Generalija Investments in Fakultete za upravo UL.**

Osrednje teme letošnje konference bodo tudi:

- **Informacijska varnost in zasebnost**
- **Varstvo osebnih podatkov se prepleta z vrsto področij**
- **Stebri odgovornega upravljanja sistemov z umetno inteligenco**
- **Umetna inteligenca v praksi**

Predstavljamo strokovnjake, ki bodo na konferenci delili svoje vpoglede, znanje in izkušnje iz prve roke:

- **Miklavž Šef,** Urad vlade za informacijsko varnost
- **Tomi Dolenc,** Arnes
- **Primož Govekar,** Info Hiša
- **Rosana Lemut Strle,** odvetnica
- **Jaka Repanšek,** Oglaševalsko razsodišče
- **Aleš Veršič,** Ministrstvo za digitalno preobrazbo
- **Maruša T. Veber,** Pravna fakulteta Univerze v Ljubljani
- **Alenka Guček, Tanja Zdolšek Draksler, Matej Kovačič,** Mednarodni raziskovalni center za umetno inteligenco, Inštitut Jožefa Štefana
- **Karlo Paljug,** Zagrebačka banka
- **Martin Možina,** Mercator
- **Andraž Istenič,** SRC Rešitve za zdravstvo
- **Franc Bračun,** NLB

Program konference in prijava:

Mali partner: SRC Rešitve za zdravstvo

Organizatorja: InfoHiša AKADEMIJA Finance

Medijski pokrovitelj: Računalniške novice www.racunalniske-novice.com

Denuvo, ki se bori proti piratom, se bo spravil še nad žvižgače

Podjetje Iderto, razvijalec programske opreme Denuvo, ki povzroča številne skrbi piratom oziroma »crackerjem«, je naznanilo novo tehnologijo, ki bo v izredno pomoč razvijalcem, ki jih skrbi, da bodo drugi razkrili občutljive informacije o njihovi intelektualni lastnini.

Ustvarjalci protipiratske programske opreme Denuvo so nedavno razkrili novo tehnologijo TraceMark for Games, ki bo razvijalcem iger pomagala izslediti uhajanje podatkov. Podjetje Denuvo je znano predvsem po svoji programski opremi DRM, ki se uporablja v več nedavnih in prihajajočih računalniških igrah, kot so Dragon's Dogma 2, FC 25, Street Fighter 6, Star Wars Jedi Survivor, Mortal Kombat 1, Dead Space Remake in praktično vse ostale AAA igre.

Programska oprema Denuvo za upravljanje digitalnih pravic (DRM) je bila prvotno izdana leta 2014, nato pa jo je leta 2018 prevzelo podjetje Irdeto. Hitro je postala precej kontroverzna, saj je bilo Denuvo precej težko zaobiti in je ljudem učinkovito preprečevala piratiziranje in tudi goljufanje znotraj iger, krivili pa so jo tudi, da negativno vpliva na delovanje teh iger. V zadnjem času je Irdeto svoj domet razširil tudi izven iger za osebne računalnike. Z lanskim letom smo prvič dobili Switch igre, ki jih je ščitil Denuvo.

Odslej bodo lažje odkrili žvižgače

Medtem ko se uspešno spopadajo s pirati, so svoje moči usmerili še v žvižgače. TraceMark je tehnologija vodnega žiga, ki razvijalcem omogoča dodajanje edinstvenih in nevidnih identifikatorjev za določene datoteke. V primeru, da bi igre ali določene datoteke zašle na splet, bi lahko s temi identifikatorji razvijalci prepoznali, kdo je bil v tem primeru žvižgač, morebiti interni zaposleni, vplivnež, Youtube ustvarjalec ali kdo drug. V podjetju so prepričani, da je to ogromen korak naprej za zaščito občutljivih informacij na področju gaminga. Podatki so še posebej občutljivi tik pred izidom igre, ko jo razvijalec začne deliti med ožjo skupino uporabnikov, bodisi zaradi testiranja ali priprave vsebine za izdajo.

Njihova primarna programska oprema bo vedno v konfliktu z vsaj eno skupino uporabnikov. TraceMark pa vsaj na prvi pogled deluje pozitivno za celotno gaming industrijo. Uhajanje in kraja podatkov lahko za seboj pustita resne posledice za razvijalca in studio. Število tovrstnih primerov v zadnjih letih konstantno narašča. Primeri so več kot zgovorni: informacije o lokaciji dogajanja igre Fallout 4 in tudi samo zasedbo je razkril kar spletni portal Kotaku; podrobnosti o zgodbi igre The Last of Us Part 2 so na splet zašle nekaj mesecev pred izidom igre; pred dvema letoma je iz rok studia Rockstar Games ušlo več kot 90 posnetkov najnovejše igre GTA 6; razvijalec Insomniac pa je izgubil še več: 1 TB podatkov o vseh načrtovanih projektih, zgodnjo različico igre Wolverine, osebne podatke zaposlenih …

V primerih kibernetskega napada najverjetneje tudi tehnologija TraceMark ne bo uspela rešiti zagate razvijalcev. Bolj je namenjena za načrtno uhajanje podatkov tistih, ki so dobili zgoden dostop do občutljivih materialov.

					AVTOR: BOTY	POMLADNI MESEC	IT. SOPRANISTKA (MIRELLA)	LEGENDARNI BOBNAR BEATLOV	PREDMOLIVEC V MOŠEJI	SAMURAJSKI MEČ	MAŠČOBNA OBLOGA V ŽILAH
					ČELINA JUŽNO OD EVROPE						
					NAJBOLJ RAZVIT SESALEC					4	
					NORVEŠKA FILMSKA IGRALKA REINSVE						
					ŠVEDSKI REŽISER BERGMAN						
1	2	3	4	5	DETE						
:DRUŽINSKI ZABAVNIK	ODSTOPNA PRAVICA	MINERAL	VPREGA Z ENIM KONJEM	STAN IN ... / BRIT. REŽ. MENDES					NINA OSENAR / LASTNIK RANČA		
ZAPOR, JEČA						NAŠA PEVKA BOTO	NELAGODEN OBČUTEK / VAROVALNA PRIPRAVA				5
GLAVNO MESTO ROMUNIJE										BLAGAJNA	OTOK V OTOČJU TUAMOTU
PREBIVALKA KRAJA ADAMOVO		3									
NATAŠA NANEVA			GORA NAD LOGARSKO DOLINO (2350 M)	PREBIVALEC KAIRA / AM. ASTRONAVT ARMSTRONG							
KANADSKA POPEVKARICA (CELINE)					JEZERSKA USEDLINA	ZAČRTENA SMER / ČASOPISNI OGLAS, ANONSA			2		
PUŠKINOV LITERARNI JUNAK (JEVGENIJ)								EG. BOG SONCA / PETELINJI BOJ			
NASILNEŽ									NIT (POMANJŠEVALNO)	SLOVENSKI BIATLONEC FAK	DOGOVORJENA MERSKA KOLIČINA
:DRUŽINSKI ZABAVNIK	SLOVENSKI ODBOJKAR (ALEN)	TLESK / REKA SKOZI FIRENCE									
NAREČNO IME ZA LOČEK				NIKALNICA / GORSKI DROBIR, SIPEC			FRANCOSKI PISATELJ (BORIS) / SL. PEVKA DEŽMAN				
UKRAJINSKI POLOTOK				1	SLOVENSKI SOCIOLOG MOČNIK / JANEZ ERŽEN						
ZAŠČITENA GORSKA CVETICA, SVIŠČ								ALPSKA DOLINA POD TRIGLAVOM			
ŽENSKA VEČERNA OBLEKA								AMERIŠKA PEVKA MAX			

FRENI: it. sopranistka, **ABANDON:** odstopna pravica, **VIAN:** fr. pisatelj, **INSERAT:** anonsa, **IMAM:** predmolivec v mošeji

NAGRADE in NAGRAJENCI

Med reševalce, ki bodo do petka, **12. 4. 2024,** poslali pravilno rešitev, bomo z žrebom razdelili privlačne nagrade:

3x sledilnik predmetov Chipolo

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**

Sebastjan Hasaj, Maribor: USB ključ Apacer AH350 128 GB 3.1

Eva Cankar, Col: USB ključ Apacer AH350 128 GB 3.1

Uroš Kristan, Žiri: USB ključ Apacer AH350 128 GB 3.1

Nagrade podarja podjetje Stromboli, d.o.o.

Rešitev križanke 4/XXIX: GRAFI

LINUX BEYBA™

KOLEDAR

DOGODEK	TERMIN	PRIJAVE
BREZPLAČNO USPOSABLJANJE: PRILOŽNOSTI IN OBVEZE DIGITALNE DOSTOPNOSTI ZAVOD ZA DIGITALNO DOSTOPNOST A11Y.SI	9. 4. 2024	www.digitalnadostopnost.si/o-nas
PANDORINA SKRINJICA DIGITALIZACIJE V INDUSTRIJI SMART COM D.O.O.	10. 4. 2024	www.smart-com.si/pandorina-skrinjica-digitalizacije
DIGIDAN DIMA CENTER D.O.O.	10. 4. 2024	www.digidan.si
ZAUH 2024 PALSIT D.O.O.	11. 4. 2024	zauh.palsit.com
SLOVENSKI KADROVSKI KONGRES PLANET GV D.O.O.	11.–12. 4. 2024	skkongres.si
FORUM PODATKOVNE ANALITIKE PLANET GV D.O.O.	25. 4. 2024	www.planetgv.si/forum-podatkovne-analitike/

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

Sodelavci in novinarji:
Maja Lavrač, Matej Saksida, Peter Čebron
Blaž Ulaga, Jana Breznik, Jan Sladič in
Matej Komprej

Fotografije:
Arhiv Računalniške novice

Tisk:
Tiskano v Sloveniji

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

Oblikovanje in DTP:
Tanja Kaštrun 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.

Sporočila za javnost sprejemamo na Rn@stromboli.si

Izdaja revije je finančno podprla Javna agencija za raziskovalno dejavnost Republike Slovenije.

To je novi

HP EliteBook 655 G10

napredenjši s procesorjem AMD Ryzen™

Na tekočine odporna tipkovnica z osvetlitvijo

Procesor AMD Ryzen™ 5 7530U

do 4,5 Ghz

Vaša opravila bodo opravljena v hipu.

Vgrajen NVMe™ s kar

512 GB

Za brezksrbno in hitro nalaganje vaših vsebin.

Fotoaparat z visoko ločljivostjo

Velikost zaslona

15,6”

Full HD

816W6EA

Velik nabor priključkov

Pomnilnik

16 GB

DDR4-3200 MHz

Izjemno varen in cenovno ugoden računalnik HP EliteBook 655, ki ga je enostavno upravljati in vključuje najnovejši procesor AMD Ryzen™, nudi možnosti povezovanja ekip in nastavljive priključke, ki jih potrebujejo, da so lahko produktivne v pisarni, doma in na poti.

Cena modela

1.184,62 €

Cena vključuje DDV.

Za vse ostale informacije obiščite

www.src.si/hp-amd-ponudba


Danfoss – izbrani partner
za pomoč strankam pri **razogljičenju.**
ENGINEERING
TOMORROW
Danfoss