



IT u fabrikama i velikim sistemima

Fabrike nove ere

Zamislite fabriku u kojoj proizvodi nastaju gotovo bez ljudske intervencije. Ne samo da roboti sklapaju robu, nego i komuniciraju međusobno, optimizuju procese u realnom vremenu, a veštačka inteligencija predviđa kvarove pre nego što se dogode. Nema više zastoja u proizvodnji, nema viškova niti manjkova sirovina ili zaliha... sve je sinhronizovano i efikasno. Dobro došli u eru Industrije 4.0!

 Dejan Ristanović

Termin „Industrija 4.0“ označava četvrtu industrijsku revoluciju, koja se temelji na digitalizaciji i povezivanju proizvodnih sistema. Prvu industrijsku revoluciju donela je parna mašina, drugu masovna proizvodnja uz pomoć električne energije, treću uvođenje elektronike i automatizacije, a sada smo duboko zaronili u četvrtu revoluciju, koju karakterišu Internet stvari (IoT), veštačka inteligencija (AI), mašinsko učenje, *big data* modeli i, kao kruna svega, napredni roboti

Cilj Industrije 4.0 nije samo da mašina zameni čoveka, već da se proizvodnja učini pametnom – sistem koji samostalno donosi odluke, prilagođava se promenama i optimizuje rad u hodu. Takva proizvodnja je efikasnija, fleksibilnija i znatno brže reaguje na potrebe tržišta.

Robotizacija je više od mehanike

Industrijski roboti više nisu samo mehaničke ruke koje ponavljaju jednostavne zadatke. Nisu čak ni ruke

opremljene senzorima, kamerama i mašinskim vidom. Oni, uz sve pomenuto, imaju „pamet“ ili su povezani sa centralnim sistemima koji analiziraju njihove podatke i „misle“. Pojavljuju se i kolaborativni roboti (coboti) koji bezbedno sarađuju sa ljudima u istom radnom prostoru.

Roboti se danas koriste u montaži, zavarivanju, pakovanju, farbanju, ali i u preciznim operacijama koje zahtevaju milimetarsku preciznost. Njihova fleksibilnost omogućava brzu



promenu proizvodnih linija, što je ključno u vremenu kada se proizvodni ciklusi skraćuju, a personalizacija proizvoda postaje standard.

Pametna fabrika na delu

Srce pametne fabrike čini mreža senzora, aktuatora, kontrolera i softvera. Svaka mašina, linija ili alat ima ugrađene IoT uređaje koji prikupljaju podatke – o temperaturi, vibracijama, brzini, pritisku, protoku...

Ti podaci se šalju centralnim sistemima za obradu, često u *cloud*-u, gde ih algoritmi analiziraju u realnom vremenu.

Komunikacija se odvija preko industrijskih mreža – najčešće preko *Ethernet/IP*, *PROFINET*, *Modbus TCP* ili *OPC UA* protokola. Tu su i bežične tehnologije – *Wi-Fi*, *5G* i *LoRaWAN* – koje omogućavaju povezivanje mobilnih robota, autonomnih vozila i udaljenih senzora. Svi ti podaci bili bi beskorisni bez upravljačkih sistema – programabilnih logičkih kontrolera (PLC), industrijskih PC računara i SCADA sistema. PLC kontroliše rad pojedinačnih uređaja na liniji, dok SCADA nadgleda čitave procese i omogućava ljudima da interveniše kada je potrebno.

Softverski alati za digitalne blizance (*digital twins*) omogućavaju simulaciju čitavog proizvodnog procesa u digitalnom obliku, pre nego što se fizički izvede. To smanjuje rizike, ubrzava planiranje i omogućava precizno testiranje optimizacija.

AI u službi proizvodnje

Veštačka inteligencija u fabrikama postaje mozak čitavog sistema. AI može da analizira podatke sa senzora, predvidi kada će doći do zastoja, prati nabavku robe i eventualni „mrtvi hod“, pa da svemu tome automatski prilagodi parametre rada mašina ili čak optimizuje raspored zaposlenih.

AI može da uoči nepravilnosti u radu motora pre nego što se pojavi kvar, predloži optimalan raspored sirovina ili, uz pomoć proširene stvarnosti, pomogne tehničarima u dijagnostici,



menjajući čitav proces tako da bi se, čak i u slučaju nekog zastoja, koristile mašine koje su i dalje u punoj funkciji. Cilj je jasan: učiniti proizvodnju efikasnijom i optimizovati troškove.

Ekonomija i radna mesta

Jedno od najčešćih pitanja koje se postavlja u vezi sa Industrijom 4.0 jeste: šta će biti sa radnim mestima? Najzad, i u prvoj industrijskoj revoluciji pojavili su se ludisti koji su razbijali mašine plašeći se da će radnici ostati bez posla. Frankeštajnski sindrom je kod ljudi i danas veoma snažan.

Istina je da određeni poslovi nestaju – naročito oni rutinski, repetitivni. Kao što su nakon dolaska računara maltene nestali stenodaktilografi ili slovoslagачи. Pojavljuju se nova zanimanja: operateri za rad sa robotima, inženjeri automatizacije, analitičari podataka, specijalisti za sigurnost industrijskih mreža... „Nevolja“ je jedino u tome što ova mesta zahtevaju školovane kadrove, dok će za one koji su bili fizička radna snaga posla zaista biti sve manje.

Industrija se ne dehumanizuje – ona se transformiše. Uloga čoveka se menja: umesto da fizički izvršava zadatke, čovek postaje supervizor, analitičar i kreator. Dok i to ne pre-

uzme AI, a onda stvarno možemo da se zapitamo šta će biti sa nama.

Ekonomskim rečnikom rečeno, produktivnost po jedinici rada raste. To može značiti niže cene proizvoda, ali i veće marže za proizvođače. U početku uvođenje ovih tehnologija može biti skupo, ali dugoročno ono donosi uštede i veću konkurentnost na tržištu.

Da li će sve biti jeftinije?

U poznatom SF romanu „Golo Sunce“ koji je objavljen još 1956. godine Isaac Asimov, tvorac reči robotika, opisuje planetu koja se zove Solarija, na kojoj živi 20 ljudi i 20 miliona robota. Sve je toliko robotizovano i automatizovano da se pitanje troškova praktično i ne postavlja. Kada na planetu dolazi stranac-detektiv, oni za njega izgrade čitavu zgradu, koju će posle odlaska razoriti. Jer, kako kaže robot koji vodi tog detektiva, „Posredi je samo to što je za njih jednostavno da sagrade kuću, a i razoriti je mogu uz veoma mali napor“. Da li to znači da će, kada Industrija 4.0 dostigne svoje vrhunce, roba biti praktično besplatna?

Paaaa... ne baš. Kod potrošačkih proizvoda koji nastaju u velikim količinama – kao što su telefoni, tele-

Četvrtu industrijsku revoluciju karakterišu Internet stvari, veštačka inteligencija, mašinsko učenje, big data modeli i, kao kruna svega, napredni roboti

Softverski alati za „digitalne blizance“ omogućavaju simulaciju celog proizvodnog procesa u digitalnom obliku, pre nego što se fizički izvede



BUDUĆNOST KOJA JE POSTALA STVARNOST

Siemens Amberg (Nemačka) Jedan od najpoznatijih primera Industrije 4.0 u praksi je *Siemens*-ova fabrika u Ambergu, gde se proizvode automatski kontroleri, za šire tržište ali posebno za druge pametne fabrike. Automatizacija je prešla 75% svih procesa: roboti, IoT senzori i AI analizatori konstantno prate kvalitet, efikasnost i stanje opreme. Greške su gotovo iskorenjene – stepen tačnosti je neverovatnih 99.99885%. Ljudi i mašine ovde direktno sarađuju, bez potrebe za ogradama ili fizičkom separacijom.

Tesla Gigafactory (SAD, Kina, Nemačka) Kompanija Tesla je redefinisala pojam automatizovane proizvodnje u automobilske industriji. Njene giga fabrike u Nevadi, Šangaju i Berlinu koriste hiljade robota – uključujući robusne KUKA robotske ruke koje vare, montiraju, boje i testiraju automobile, ali i proizvode

baterije. Ključna razlika u odnosu na klasične fabrike je u potpunom povezivanju mašina, vozila i skladišta u jedan digitalni sistem. AI se koristi za optimizaciju toka materijala, prediktivno održavanje i planiranje resursa u realnom vremenu.

Foxconn (Kina) Najveći svetski proizvođač elektronike, poznat po sklapanju *iPhone* uređaja, uveo je desetine hiljada robota u svoje pogone. Projekat pod imenom *Foxbot* doveo je do toga da određeni delovi proizvodnje funkcionišu gotovo bez ljudske intervencije. Kompanija je najavila da će do kraja decenije transformisati više od 30% proizvodnje u potpuno automatizovanu.

ABB Smart Factory (Švedska) ABB je u Vasterasu otvorio potpuno automatizovanu fabriku koja koristi robote – za pravljenje robota. Ovde svaki proizvod-

ni modul komunicira sa centralnim AI sistemom, a proizvodni podaci se analiziraju kako bi se proces neprestano poboljšavao. Eto primera fabrike gde se granice između digitalnog i fizičkog sveta brišu.

BMW Group Plant (Nemačka, Mađarska) BMW je implementirao digitalne blizance za gotovo svaku proizvodnu liniju u svojim najnovijim fabrikama. U pogonu u Debrecinu u Mađarskoj, koji će biti otvoren ove godine, celokupan sistem biće zasnovan na konceptu *digital-first*. To znači da će proizvodnja prvo biti isplanirana, testirana i optimizovana u digitalnom okruženju, pa tek onda fizički izvedena. Sve proizvodne jedinice biće međusobno povezane i samostalno prilagođavati radne parametre u zavisnosti od modela automobila koji se pravi.

vizori, automobili – cene mogu pasti zahvaljujući većoj efikasnosti i manjoj količini otpada. Ali s obzirom na sve veće zahteve za personalizacijom i bržim ciklusima isporuke, može doći i do rasta cena kod proizvoda u malim serijama, jer se plaća brzina, prilagodljivost i održivost.

Industrija 4.0 ne garantuje „masovnu jeftinoću“, već optimizaciju vrednosti – za proizvođača i potrošača.

Standardi i bezbednost

Povezivanje svih sistema ne bi bilo moguće bez standardizacije. Organizacije poput IEEE, ISO i OPC Foundation definišu pravila i protokole kojima se osigurava interoperabilnost različitih uređaja i proizvođača.

Digitalizacija donosi i mnoge pretnje – sajber bezbednost postaje ključna tema. Napadi na fabrike nisu više

fikcija – realni su i mogu naneti ogromne štete. Zbog toga se sve više koristi *zero trust* pristup, enkripcija podataka, autentikacija uređaja i kontinuirano praćenje mrežnog saobraćaja.

Budućnost koja je već stigla

U mnogim razvijenim zemljama implementacija Industrije 4.0 već je u poodmakloj fazi. Kompanije kao što su *Siemens*, *Bosch*, GE i ABB nude kompletna rešenja koja obuhvataju sve – od senzora, preko softvera, do AI sistema. U Srbiji se takođe pojavljuju pilot-projekti i inicijative, naročito u automobilske i prehrambenoj industriji, kao i u saradnji sa univerzitetima.

Industrija 4.0 nije samo tehnološki trend – ona je suštinska promena načina na koji proizvodimo, radimo i posluje. Donosi prilike za rast, ali i izazove za prilagođavanje. Ključ uspeha biće u spremnosti da se uči i inovira. Fabrika budućnosti nije samo puna robota... već i pameti. Prirodne kao i veštačke.

Uloga čoveka se menja: umesto da fizički izvršava zadatke, čovek postaje supervizor, analitičar i kreator. Dok i to ne preuzme AI, a onda stvarno možemo da se zapitamo šta će biti sa nama





naših 30 godina

Tehnologija, ljudi i vizije

**Ljudi koji su stvarali
PC i njihovi doživljaji u
računarskom svetu**

**Rast i razvoj domaćeg
računarskog tržišta
kroz vizuru vodećeg
IT časopisa**

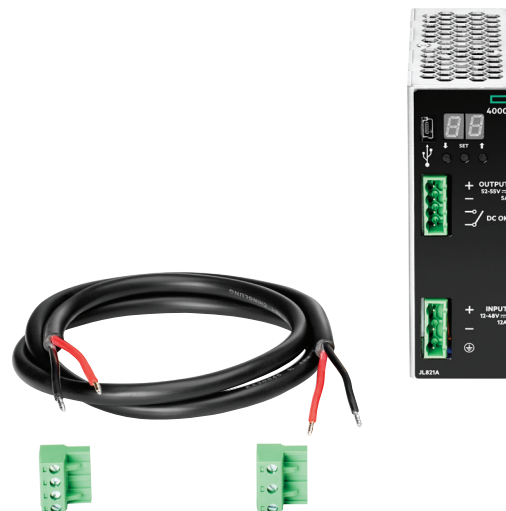
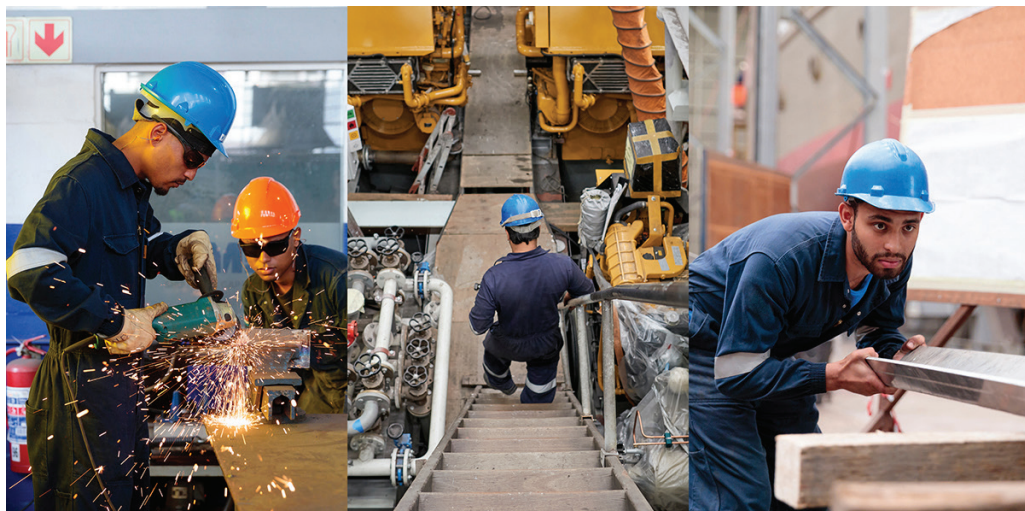
**25 priča
sa tehnološke ivice**

Monografija na 480 strana štampana u vrhunskoj tehnici
ukrasiće vašu biblioteku.

U prodaji
pcpress.rs

Mreže koje povezuju industriju

Industrija se menja. Sve je brže. Sve je povezano. Podaci su nova valuta. U tom svetu, mreža je krovotok. Stabilna, sigurna i pametna. Kako HPE Aruba Networking radi u industrijskom okruženju Srbije



HPE Aruba Networking je stub nove industrijske komunikacije. U Srbiji, HPE Aruba Networking mreže već rade u fabrikama nameštaja, u pogonima drvne industrije, hemijskoj i prehrambenoj proizvodnji. I svuda gde su povezivanje i automatizacija ključ uspeha.

Zašto HPE Aruba Networking?

HPE Aruba Networking nudi više od povezivanja. To je platforma. Otvorena. Bezbedna. Fleksibilna. Ona povezuje ljude, mašine i procese.

Posebno mesto zauzimaju HPE Aruba Networking industrijski switch

Industrijski korisnici danas žele jednu stvar: da sve radi. Bez obzira na brend uređaja, HPE Aruba Networking to omogućava

uređaji – serije 4000i i 4100i. Otporni su na ekstremne uslove, na prašinu, vlagu i visoke temperature. Namereni su za rad u industrijskim okruženjima. Mogu se montirati u ormare, na zidove ili direktno u proizvodni pogon, podržavaju PoE napajanje, integraciju s nadzornim sistemima, prioritizaciju saobraćaja i lako je upravljati njima kroz Aruba Central.

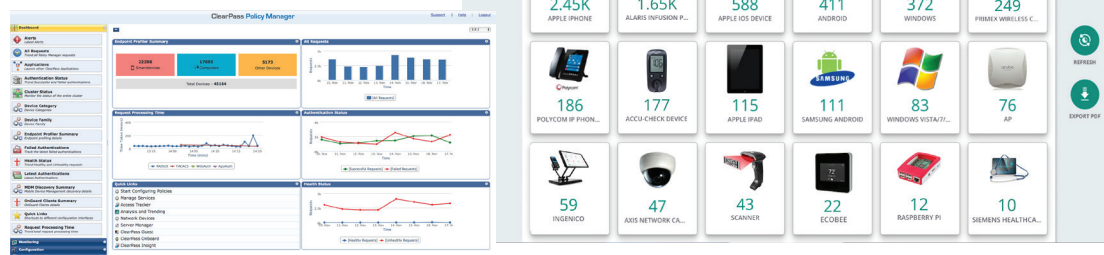
Industrijski access point (AP) uređaji iz HPE Aruba Networking portfolija pružaju izuzetnu pokrivenost u

izazovnim okruženjima. HPE Aruba Networking AP uređaji za spoljašnju i industrijsku primenu dizajnirani su za okruženja gde drugi Wi-Fi sistemi otkazuju. Otporni su na udarce, temperaturne oscilacije i elektromagnetne smetnje. Pokrivaju velike hale, povezuju pokretne radne jedinice, nude sigurnost enterprise klase, a dolaze sa integrisanim analitikama.

HPE Aruba Networking mreže omogućavaju rad u realnom vremenu, povezujući senzore, kamere, robote, mašine i ljude. Sve to bez zastoja u radu. Bez kompromisa. Bez rizika.

U raznim industrijama

Industrijski korisnici danas žele pre svega jednu stvar: da sve radi. Bez obzira na brend uređaja, HPE Aruba Networking upravo to omogućava. Njeni uređaji se savršeno integrišu sa sistemima kao što su Zebra čitači i štampači, SCADA sistemi i PLC kontroleri. Kako sa cloud tako i sa on-premise rešenjima.



Prepoznata je i u industriji pokućstva. Tamo HPE Aruba Networking upravlja celokupnom internom logistikom. Povezuje skladište, linije i administraciju. Omogućava bežično skeniranje, mobilnu štampu i online pristup dokumentaciji. Bez pada mreže. Bez zastoja.

U drvenoj industriji HPE Aruba Networking se koristi u kombinaciji sa IoT senzorima. Mreža pokriva hale za sušenje, linije za obradu i skladišta. Pomoću HPE Aruba Networking platforme korisnici prate temperaturu, vlagu, prisustvo radnika i stanje mašina. Sve to u realnom vremenu.

Hemijska industrija ima stroge zahteve. HPE Aruba Networking ih ispunjava sve. Ugrađena redundansa. Napredna segmentacija mreže. Detekcija pretnji u realnom vremenu. HPE Aruba Networking ClearPass i Aruba Central zajedno pružaju potpunu kontrolu i uvid u svaki deo mreže.

U prehrambenoj industriji HPE Aruba Networking se koristi za praćenje proizvodnih procesa. Integracija sa SCADA sistemima omogućava detaljan nadzor. Svaka mašina je povezana. Svaki paket se prati. Kvalitet se meri i arhivira automatski.

Otvorena arhitektura

Zajednički imenilac? Otvorena arhitektura. HPE Aruba Networking je napravljena da se povezuje. Bez obzira na to da li je Zebra uređaj, senzor za temperaturu, PLC ili SCADA nadzorni sistem. HPE Aruba Networking se ne boji različitosti. Ona je most.



U industriji, stabilnost je sve. A HPE Aruba Networking koristi napredne algoritme za balansiranje saobraćaja. Automatsko preusmeravanje, prepoznavanje prioriteta. Video-nadzor ima svoj kanal. Sve radi, čak i kada nešto ne radi.

Aruba Central je mozak sistema. Jedna tabla. Jedan pogled. Sve lokacije. Sve mreže. Sve što se dešava – prikazano jasno. U realnom vremenu, s mogućnošću analize, automatizacije i optimizacije.

Osetljivi industrijski sistemi imaju potrebu za upravljanjem pristupom? HPE Aruba Networking ClearPass. Pravi korisnik. Pravo vreme. Prava prava. Segmentacija po uređaju. Po lokaciji. Po tipu korisnika. Bezbednost je ugrađena, ne dodata.

Implementacija i podrška

A implementacija? Brza i skalabilna. HPE Aruba Networking uređaji se

Ugrađena veštačka inteligencija prati tokove saobraćaja, analizira i predlaže promene. Uči iz ponašanja mreže. Otkriva potencijalne probleme pre nego što se dese

Zajednički imenilac je otvorena arhitektura. HPE Aruba Networking je napravljena da se povezuje

konfigurišu unapred – Zero Touch Provisioning. Donose se spremni. Povezivanje je intuitivno. Sve je u Aruba Central platformi.

Podrška? Lokalna. Prisutna. Stručna. HPE Aruba Networking partneri u Srbiji imaju iskustvo u raznim industrijama. Znaju šta znači proizvodnja 24/7. Reagovanje je brzo. Rešenja su testirana.

HPE Aruba Networking ne staje. Ona uči. Ugrađena veštačka inteligencija prati tokove saobraćaja, analizira i predlaže promene. Uči iz ponašanja mreže. Otkriva potencijalne probleme pre nego što se dese.

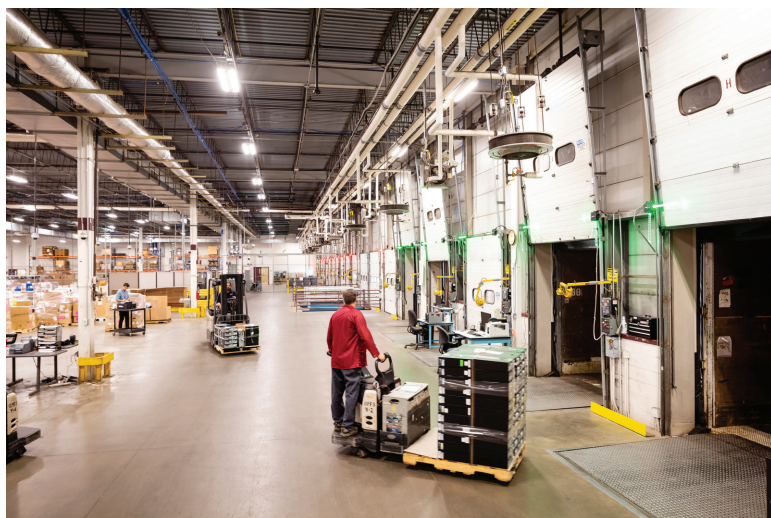
Industrija budućnosti

Industrija budućnosti je već tu, a HPE Aruba Networking je njen deo. S više hiljada uređaja u pogonu. S više miliona paketa u sekundi. Sa stabilnošću koja ne trpi izgovore. HPE Aruba Networking nije samo mreža. Ona je platforma za digitalizaciju industrije, za pametnu proizvodnju i, pre svega, konkurentnost u vreme trendova koji se često menjaju.

Povezivanje. Vidljivost. Bezbednost. Automatizacija. To je HPE Aruba Networking. To je industrija. To je Srbija – spremna za sledeći korak.

Za pitanja u vezi sa HPE Aruba Networking ponudom, obratite se lokalnom stručnjaku Dejanu Džodanu na d.dzodan@selectium.com.

 hpe.com



Cyber bezbednost: pouzdan štit za kompanije svih profila u savremenom digitalnom okruženju

Dok kompanije u Srbiji ubrzano digitalizuju poslovanje, globalni trendovi reflektuju alarmantnu stvarnost: 43 odsto svih cyber napada cilja upravo MSP sektor (Verizon 2024)

Istraživanje Sophos-a potvrđuje da 68 odsto MSP-a u Evropi doživi ozbiljan sigurnosni incident na godišnjem nivou, a prosečni trošak oporavka za firmu od 50 zaposlenih iznosi oko 180.000 evra. Ovi podaci nisu samo statistika – oni su crvena lampica za svaki biznis koji zanemaruje „digitalnu higijenu“. Ranjivost MSP sektora nije slučajna. Hakere privlači kombinacija kritičnih podataka (finansijski podaci, lični podaci klijenata) i često nedovoljno zaštićene infrastrukture.

„MSP su postale „tramvajska stanica“ za hakerske napade na veće kompanije. Na primer, kada napadi ugroze dobavljača jedne kompanije, automatski dobijaju pristup celoj njegovoj mreži klijenata“, objašnjava Jelena Petrović, direktorka prodaje kompanije PULSEC, regionalnog lidera u cybersecurity oblasti.

Veličina organizacije nije merilo bezbednosti – ključ je u stepenu zaštite

Nedostatak specijalizovanog IT osoblja, neadekvatna primena bezbednosnih protokola i nedovoljna edukacija zaposlenih o digitalnim pretnjama dodatno povećavaju rizik. Posledice uspešnog cyber napada mogu biti razarajuće: od gubitka osetljivih podataka i finansijskih prevara, preko



prekida poslovanja i narušavanja poverenja klijenata, do skupih pravnih sporova i kazni zbog nepoštovanja propisa o zaštiti podataka.

Digitalna bezbednost više nije opcija, već imperativ. Ne radi se samo o instaliranju antivirusnog softvera; potrebna je sveobuhvatna strategija koja uključuje zaštitu podataka, aplikacija, mreža i radnih stanica, uz kontinuirano upravljanje ranjivostima i brz odgovor na incidente. Za sve organizacije koje žele da zaštite svoje poslovanje korisno je da shvate da je proaktivna odbrana daleko isplativija od reaktivnog saniranja štete.

„Najuspešnije kompanije su svesne činjenice da cyber bezbednost zahteva partnerski pristup – kombinaciju tehnologije, ljudi i procesa, koja prevazilazi njihove interne kapacitete. Najčešći scenario koji vidimo? Vlasnik kompanije nas zove kada je već kasno – nakon što je ransomware šifrovao sve servere. Traumatično je gledati kako firma koja uspešno posluje 20 godina gubi sve podatke jer nisu imali ni osnovni backup. Prava zaštita počinje pre incidenta: 24/7 nadzor, kao što pruža naš SOC, otkriva sumnjive aktivnosti u zaraznom stadijumu. Kada naši analitičari primete da se neki uređaj

ponaša drugačije od uobičajenog ili da se neko neovlašćeno kreće kroz mrežu – intervenišemo pre nego što hakeri izvedu glavni napad. To je razlika između ručno sastavljenog alarma i profesionalnog sistema za ranu detekciju požara“, naglašava Jelena Petrović, direktorka prodaje u PULSEC-u, najvećoj regionalnoj *cybersecurity* kompaniji.

Kroz strateško partnerstvo s Telekomom, PULSEC donosi MSP sektoru pakete koji odgovaraju na sledeće izazove:

CyberSecurity paketi – zaštita bez kompromisa

Klijentima su na raspolaganju četiri paketa: *Endpoint Security*, *Net Security*, *Backup&Recovery* i SOC paketi. Nezavisno od odabranog nivoa zaštite u okviru *Net Security* ili *Endpoint Security* paketa, pružamo vam neprekidnu podršku i nadzor tima iz najvećeg bezbednosno-operativnog centra (SOC) na tržištu. Naš tim će pratiti vaš sistem 24/7, detektovati i reagovati na sve potencijalne pretnje u realnom vremenu, osiguravajući zaštitu bez prestanka.

Endpoint Security – prva linija odbrane!

Uz naša *Endpoint Security* rešenja, vaši uređaji su zaštićeni 24/7, a vi bezbrižno posluje, sigurni od *cyber* pretnji. Naša rešenja nude tri nivoa zaštite – *Basic*, *Advanced* ili *Premium*



Jelena Petrović,
direktorka prodaje
kompanije PULSEC

– tako da klijenti mogu da izaberu tačno onoliko zaštite koliko smatraju da je potrebno, pri čemu svi paketi uključuju EDR i naprednu zaštitu od malvera. Na raspolaganju smo i za prilagođavanje paketa, kao i da se klijenti opredele za rešenja renomiranih vendora.

Net Security – neprobojni štit za vašu mrežu!

Ojačajte bezbednost uz napredna *firewall* rešenja! Blokirate neovlašćene pristupe, filtrirajte saobraćaj i zaštitite svoje podatke 24/7. Bezbednost i stabilnost vaše IT infrastrukture počinju ovde! Mreža naših klijenata postaje sigurna od prvog koraka zahvaljujući *Palo Alto NGFW firewall*-u, koji godinama dominira *Gartner*-ovim rangiranjima i efikasno štiti vašu infrastrukturu.

PULSEC nudi sveobuhvatnu zaštitu 24/7, koja obuhvata monitoring i detekciju, *Threat Hunting*, *Incident Response*, *Vulnerability Management*, *Pentesting* i programe obuka za podizanje svesti o *cyber* bezbednosti za zaposlene

Backup & Recovery – sigurnost podataka

Zaštitite važne poslovne podatke i obezbedite nesmetan rad svoje firme uz pouzdana rešenja za *backup* i oporavak. Lako za korišćenje, omogućava brz povrat podataka i pruža sigurnost – bez gubitaka i zastoja. Podaci se mogu čuvati u *cloud*-u ili na lokalnim serverima, uz mogućnost da ostanu unutar zemlje, u skladu s bezbednosnim i regulatornim zahtevima. *Backup* smanjuje rizik od gubitka podataka, štedi resurse i optimizuje troškove poslovanja.

SOC

– neprekidna zaštita 24/7

SOC ili bezbednosno-operativni centar, pruža uvid u realnom vremenu u stanje bezbednosti celokupnog informacionog sistema i služi sprečavanju, otkrivanju, analiziranju i brzom reagovanju na incidente *cyber* bezbednosti. Čine ga ljudi, procesi i tehnologija za kontinuirano praćenje i poboljšanje bezbednosnog položaja vaše organizacije.

„Najveća greška je čekati da incident postane konstantna lekcija. U savremenom poslovnom svetu, nužno je da kompanije budu proaktivne u svom razvoju, bilo da je reč o manjim ili većim organizacijama. PULSEC nudi sveobuhvatnu zaštitu 24/7, koja obuhvata monitoring i detekciju, *Threat Hunting*, *Incident Response*, *Vulnerability Management*, *Pentesting* i programe obuka za podizanje svesti o *cyber* bezbednosti za zaposlene. Naš georedundantni bezbednosno-operativni centar obezbeđuje neprekidnu zaštitu i najviši nivo dostupnosti usluga za naše klijente“, zaključuje gospođa Jelena Petrović, direktorka prodaje kompanije PULSEC, najveće regionalne *cybersecurity* kompanije.

Proverite pakete prilagođene MSP sektoru: <https://mts.rs/Poslovni/Cyber-bezbednost> Ili zakažite konsultacije za besplatnu procenu ranjivosti. U eri digitalne zavisnosti, *cyber* zaštita nije trošak, već osnova poslovnog opstanka.

 pulsec.com



Zašto je modernim industrijskim objektima neophodan uptime?

Schneider Electric, globalni lider u energetici i automatizaciji, nudi vrhunska rešenja koja osiguravaju neprekidno napajanje proizvodnih procesa i pouzdano funkcionisanje IT sistema, omogućavajući industrijskim objektima da rade bez zastoja i maksimalno efikasno

 Aleksandar Bukva, Key Account Manager Secure Power, SE

U današnjem svetu, gde je kontinuitet poslovnih i proizvodnih procesa ključan za uspeh, pouzdano napajanje i efikasna IT infrastruktura predstavljaju osnovu svakog modernog industrijskog pogona. *Schneider Electric*, globalni lider u energetici i automatizaciji, nudi vrhunska rešenja koja osiguravaju neprekidno napajanje proizvodnih procesa i pouzdano funkcionisanje IT sistema, omogućavajući industrijskim objektima da rade bez zastoja i maksimalno efikasno.

Investirajte u budućnost vaše fabrike sa Schneider Electric rešenjima IT infrastrukture

aplikacija, od manjih proizvodnih linija do velikih industrijskih postrojenja. S naprednim tehnologijama i visokim nivoom efikasnosti, *Schneider Electric* UPS sistemi pružaju:

- **Modularnost** – lako instalirajući trofazni UPS koji pruža vrhunske performanse za *data* centre i kritičnu infrastrukturu u komercijalnim i industrijskim objektima.
- **Efikasnost** – rešenja sa efikasnošću do 99% u *eConversion™* modu i brzim proširenjem kapaciteta.
- **Održivost** – visokoefikasna, modularna trofazna UPS zaštita sa fleksibilnim operativnim modovima, idealna za sve kritične aplikacije.

UPS u fabrici

Upotreba UPS uređaja u fabrikama donosi brojne prednosti koje direktno utiču na proizvodne procese i mašine:

Zaštita opreme: UPS uređaji štite proizvodne mašine i opremu od oštećenja uzrokovanih prekidima napajanja, prenaponom i drugim električnim smetnjama. Ovo produžava životni vek opreme i smanjuje troškove održavanja.

Kontinuitet proizvodnje: neprekidno napajanje osigurava da proizvodni procesi teku nesmetano, čak i u slučaju nestanka struje. Ovo je posebno

važno za industrije koje rade u neprekidnim smenama i gde svaki zastoj može dovesti do značajnih gubitaka.

Smanjenje zastoja: UPS uređaji minimiziraju rizik od zastoja u proizvodnji, što doprinosi povećanju efikasnosti i produktivnosti. Manje zastoja znači manje gubitaka i veći profit.

Povećanje sigurnosti: stabilno napajanje smanjuje rizik od nesreća i oštećenja opreme, što doprinosi sigurnijem radnom okruženju za zaposlene.

Optimizacija resursa: Sa UPS uređajima, fabrike mogu bolje upravljati svojim resursima, smanjujući potrošnju energije i operativne troškove. Ovo doprinosi održivosti i ekološkoj odgovornosti.

IT u modernim industrijskim objektima

U savremenom industrijskom okruženju, IT infrastruktura igra ključnu ulogu u unapređenju proizvodnih procesa i postizanju operativne efikasnosti. Evo nekoliko razloga zašto je IT sve prisutniji i važniji u modernim industrijskim objektima:

- **Digitalizacija proizvodnih procesa:** IT omogućava digitalizaciju i automatizaciju proizvodnih procesa, što dovodi do povećanja produktivnosti, smanjenja grešaka i optimizacije resursa.



UPS rešenja za neprekidno napajanje

Schneider Electric UPS sistemi pružaju pouzdano i neprekidno napajanje, štiteći kritične poslovne i proizvodne procese od prekida u napajanju i osiguravajući kontinuitet rada, a samim tim donose direktno smanjenje troškova, kao i smanjenje škarta, vremena za oporavak procesa itd.

UPS rešenja su dizajnirana da zadovolje potrebe različitih industrijskih



- **Praćenje i analiza podataka:** IT sistemi omogućavaju prikupljanje, praćenje i analizu podataka u realnom vremenu, što pomaže u donošenju informisanih odluka i brzom reagovanju na promene u proizvodnom okruženju.
- **Integracija s pametnim uređajima:** IT infrastruktura omogućava integraciju s pametnim uređajima i senzorima, što omogućava praćenje i upravljanje proizvodnim procesima na daljinu.
- **Sigurnost i zaštita:** IT rešenja pružaju visoku sigurnost i zaštitu podataka, štiteći industrijske sisteme od cyber napada i gubitka podataka.
- **Fleksibilnost i skalabilnost:** IT infrastruktura omogućava fleksibilnost i skalabilnost, prilagođavajući se rastućim potrebama industrijskih objekata i omogućavajući brzo prilagođavanje novim tehnologijama i tržišnim uslovima.

U današnjem dinamičnom energetskom okruženju, modernizacija postrojenja je ključna za održavanje konkurentnosti. *Schneider Electric* nudi napredna rešenja za kontrolu procesa koja omogućavaju optimizaciju performansi u realnom vremenu, smanjenje troškova i emisija, kao i prilagođavanje promenljivim tržišnim uslovima. Ta rešenja pomažu u smanjenju opterećenja opreme i povećanju efikasnosti, što je posebno važno u kontekstu sve veće integracije obnovljivih izvora energije.

IT infrastruktura za modernu industriju

U eri digitalizacije, efikasna IT infrastruktura je ključna za uspešno upravljanje proizvodnim procesima i optimizaciju resursa. *Schneider Electric* nudi sveobuhvatna rešenja za IT infrastrukturu koja uključuju:

- **Data centre i server sobe:** rešenja za data centre obezbeđuju optimalne uslove za rad servera i IT opreme, sa fokusom na energetsku efikasnost i pouzdanost.
- **Pametne mreže i automatizaciju:** integracija pametnih mreža i automatizovanih sistema omogućava vam da pratite i upravljate proizvodnim procesima u realnom vremenu, povećavajući produktivnost i smanjujući rizik od zastoja.
- **Sigurnost i zaštitu podataka:** rešenja obezbeđuju visoku sigurnost i pouzdanost IT sistema, štiteći ih od gubitka podataka.

Uspešne implementacije

Schneider Electric je ostvario brojne uspešne implementacije širom sveta, koje potvrđuju kvalitet i pouzdanost rešenja. Evo samo nekoliko primera:

- **Fabrike automobila:** implementacija *Galaxy VX* UPS sistema omogućila je neprekidno napajanje i zaštitu kritičnih proizvodnih procesa, smanjujući rizik

U savremenom industrijskom okruženju, IT infrastruktura igra ključnu ulogu u unapređenju procesa i postizanju operativne efikasnosti

od zastoja i povećavajući efikasnost proizvodnje.

- **Hemijska industrija:** *Schneider Electric* rešenja za IT infrastrukturu omogućila su integraciju pametnih mreža i automatizovanih sistema, što je rezultiralo povećanjem produktivnosti i smanjenjem operativnih troškova.
- **Energetski sektor:** implementacija naprednih rešenja za kontrolu procesa omogućila je optimizaciju performansi postrojenja, smanjenje emisija i prilagođavanje promenljivim tržišnim uslovima.

Zašto odabrati Schneider Electric?

Schneider Electric je sinonim za kvalitet, inovaciju i pouzdanost. Rešenja su rezultat decenija iskustva i stalnog unapređenja tehnologija, sa ciljem da našim klijentima pružimo najbolje moguće uslove za rad. Odabirom *Schneider Electric* rešenja, dobijate:

- **Vrhunski kvalitet:** oprema je proizvedena prema najvišim standardima kvaliteta, osiguravajući dugotrajnost i pouzdanost.
- **Podršku i servis:** tim stručnjaka je uvek tu da vam pruži podršku i pomoć, bilo da je reč o instalaciji, održavanju ili rešavanju problema.
- **Inovativna rešenja:** stalno radimo na razvoju novih tehnologija koje će vam pomoći da unapredite svoje poslovanje i ostanete korak ispred konkurencije.

Investirajte u budućnost vaše fabrike sa *Schneider Electric* rešenjima IT infrastrukture. Osigurajte neprekidno napajanje, efikasno upravljanje resursima i sigurnost vaših podataka, i postanite deo globalne mreže zadovoljnih korisnika koji veruju u kvalitet i pouzdanost *Schneider Electric*-a.

Za više informacija, posetite našu Web stranicu ili kontaktirajte s nama direktno. Naš tim je tu da vam pomogne da pronađete najbolje rešenje za vaše potrebe.

 se.com/rs

Synology ActiveProtect linija napreduje

Stalno radeći na kompaktnim rešenjima za brzo rastuća preduzeća, Synology je predstavio DP7200 za naprednu zaštitu distribuiranih sistema i DS425+, moćno ali kompaktno rešenje za efikasno upravljanje podacima



Uz digitalnu transformaciju i širenje poslovanja na više lokacija, kompanije se sve češće suočavaju sa izazovima u pogledu zaštite, dostupnosti i integracije podataka. Synology, jedan od globalnih lidera u oblasti *data management* rešenja, odgovara na ove izazove proširenjem svog portfolija s dva nova uređaja – ActiveProtect DP7200 i DiskStation DS425+.

DP7200 – centralizovana zaštita za disperzne sisteme

Kao najnoviji dodatak ActiveProtect liniji, DP7200 nudi moćnu zaštitu različitih opterećenja – od fizičkih servera i virtuelnih mašina, preko baza podataka, do Microsoft 365 naloga, na više lokacija istovremeno.

DP7200 kombinuje hardver i softver u jednom uređaju, sa ugrađenim operativnim sistemom ActiveProtect Manager, čineći ga pogodnim kao centralni menadžment server ili kao

samostalni *backup* uređaj. Uz kapacitet od 84 TB, DP7200 nudi:

- **Konsolidovan uvid u infrastrukturu** – praćenje do 150.000 radnih opterećenja i 2.500 lokacija kroz jednu kontrolnu tablu.
- **Zaštitu od ransomware napada-a i neovlašćenog pristupa** – uključujući MFA preko Active Directory, LDAP i SAML 2.0, kao i očuvanje netaknutih kopija podataka zahvaljujući imutabilnosti i izolaciji.





- **Efikasnu dugoročnu arhivu – backup** na lokaciji ili u oblaku uz deduplikaciju podataka, štedeći prostor i osiguravajući usklađenost s propisima.

DP7200 je idealno rešenje za organizacije sa distribuiranom infrastrukturom – od glavnih kancelarija, preko udaljenih poslovnica, do data centara.

Za razliku od klasičnih NAS uređaja, koji se prvenstveno koriste za deljenje i čuvanje podataka, *Data Protection Appliance* (DPA), poput DP7200, je namenski sistem razvijen isključivo za sigurnosno kopiranje i oporavak podataka. On dolazi sa unapred instaliranim softverom, optimizovanim za *backup*, replikaciju, zaštitu od *ransomware*-a i centralizovano upravljanje velikim brojem lokacija i opterećenja. DPA ne zahteva dodatne licence ili instalaciju posebnih aplikacija – sve funkcionalnosti su integrisane i spremne za upotrebu odmah po uključivanju. To ga čini izuzetno pogodnim za IT timove koji žele pouzdano i brzo rešenje bez komplikovane konfiguracije.

DS425+ – kompaktno rešenje za fleksibilne poslovne potrebe

Za timove i organizacije sa stabilnim potrebama za skladištenjem podataka, Synology predstavlja DS425+, pouzdan i snažan uređaj u kompaktnom 4-bay formatu, kapaciteta do 80 TB sirovih podataka. Uređaj nudi:

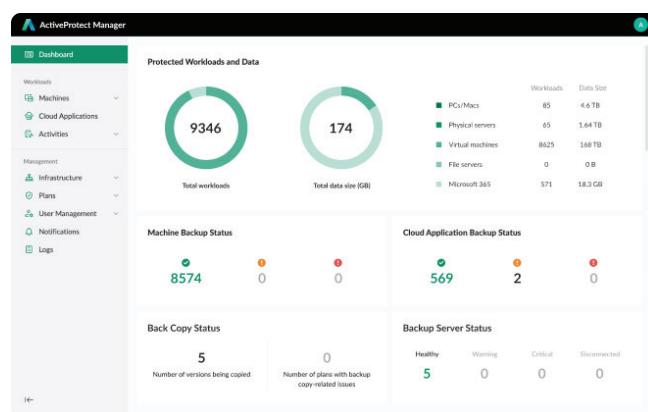
- **Poboljšanu mrežnu konektivnost** – 2.5 GbE i 1 GbE portove za brži protok podataka.
- **Podršku za NVMe uređaje** – omogućavaju keširanje i rad u *all-flash* režimu.

DPA ne zahteva dodatne licence ili instalaciju posebnih aplikacija – sve funkcionalnosti su integrisane i spremne za upotrebu odmah po uključivanju

- **Punu integraciju sa Synology softverom** – *DiskStation Manager* (DSM) nudi alate kao što su: *Synology Drive* za sinhronizaciju i privatni cloud pristup, *Active Backup Suite* za sveobuhvatnu zaštitu uređaja i cloud naloga, *Surveillance Station* za inteligentan video-nadzor.

DS425+ je posebno testiran za pouzdan rad sa Synology diskovima, uz više od 7.000 sati rigoroznog testiranja, čime se osigurava stabilan i dugotrajan rad.

Bilo da je vaša kompanija u fazi širenja ili konsolidacije IT resursa, nova Synology rešenja pružaju fleksibilnost, sigurnost i jednostavnost upravljanja koje zahtevaju savremena srednja i velika preduzeća.



DP320

Capacity: 8 TB



DP340

Capacity: 24 TB



DP7200

Capacity: 84 TB



DP7400

Capacity: 140 TB



Za više informacija posetite



<https://sy.to/pcap25> i



<https://sy.to/pcds425>

Od digitalne do društvene transformacije

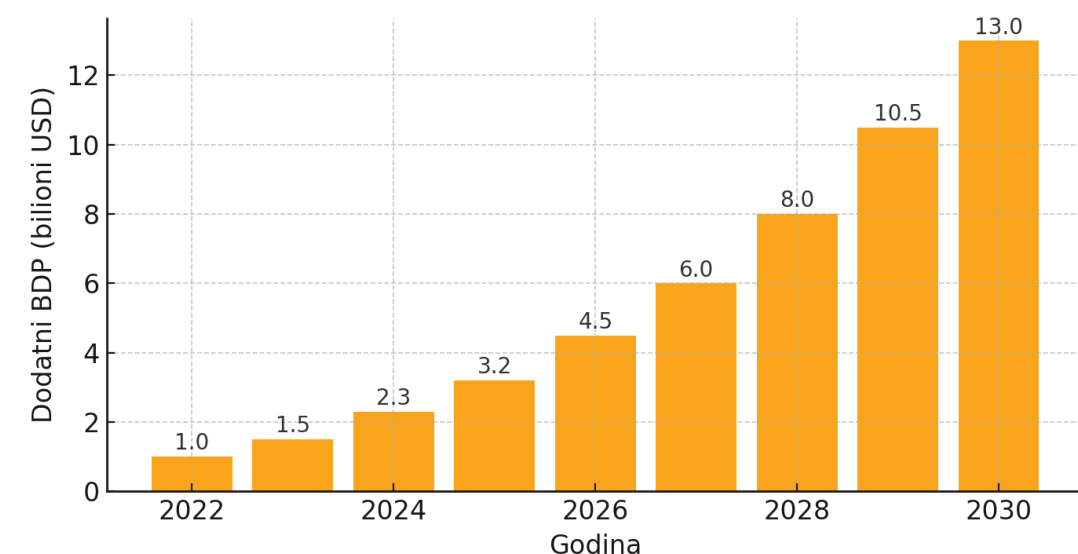
Davno smo konstatovali da ulaganja u informaciono-komunikacione tehnologije (IKT) nisu samo tehnička unapređenja, već katalizatori društvenog i ekonomskog razvoja. Sada je taj proces potpuno očigledan

U jednom gradu u jugoistočnoj Aziji, gde je pre desetak godina Internet bio luksuz a računar privilegija malobrojnih, danas mladi preduzetnici razvijaju aplikacije koje koriste milioni ljudi širom sveta. U njihovim rukama, tableti služe za udaljenu nastavu, mobilne mreže povezuju farmere sa tržištima, a lokalna klinika čuva sve zdravstvene kartone u digitalnoj bazi kojoj lekar pristupa iz bilo kog sela. Ta promena nije došla sama od sebe – bila je posledica odluke lokalne vlade i međunarodnih partnera da investiraju u IT infrastrukturu, obuku i digitalne servise.

Ovaj primer oslikava ono što analitičari sve češće naglašavaju – ulaganja u informaciono-komunikacione tehnologije (IKT) nisu samo tehnička unapređenja, već katalizatori društvenog i ekonomskog razvoja.

Brojevi koji govore

Prema Gartner-u, globalna IT potrošnja će u 2025. premašiti 5,43 biliona dolara, uz rast od 7.9% u odnosu



▲ Projekcija uticaja AI na globalni BDP do 2030 (McKinsey)

▼ Povrat na IKT ulaganja (Global Connectivity Index) – po dolaru ulaganja

na prethodnu godinu. Najveći deo tog rasta dolazi iz ulaganja u softver i *data* centre, pokretanih ekspanzijom veštačke inteligencije i generativnog AI-a. Segment *data* centara beleži najveći skok – čak 42% u odnosu na 2024, dok je softver na drugom mestu sa oko 10.5% rasta. Ovi procenti ne znače samo nove servere ili licence – iza njih stoje strateške odluke kompanija i država koje veruju da će tehnologija biti glavni izvor produktivnosti naredne decenije.

Global Connectivity Index, koji meri povezanost infrastrukture i digitalne spremnosti zemalja, pokazuje da svaki dolar uloženi u informaciono-komunikacionu (IKT) infrastrukturu u proseku donosi oko 3 dolara u BDP-u (2016), 3,7 dolara (2020), a prognoza za 2025. je i do 5 dolara povrata. Drugim rečima, ulaganje

u IT nije trošak, već multiplikator ekonomskog rasta.

Od infrastrukture do društvenih promena

Prvi talas digitalizacije bio je usmeren na hardver – kablove, bazne stanice, servere. Danas je jasno da fizička infrastruktura sama po sebi ne donosi razvoj ako je ne prate ulaganja u ljudski kapital, organizacione promene i javne politike. IDC u svojim analizama naglašava da je upravo kombinacija tehničkih i „mekih“ investicija ta koja pravi razliku – društva koja razvijaju digitalnu pismenost, unapređuju obrazovne programe i uvode digitalne javne usluge postižu dugoročno veći rast.

Upravo ta transformacija iz „kupovine opreme“ ka „građenju digitalne

Države koje žele da privuku investicije moraju ponuditi ne samo poreske olakšice, već i digitalnu infrastrukturu i regulatorni okvir koji podržava inovacije

kulture“ objašnjava zašto neke zemlje postižu izuzetne rezultate, dok druge, sa sličnim nivoom tehničke opremljenosti, stagniraju. Kada građanin može elektronski da podnese zahtev za lična dokumenta, kad poljoprivrednik u selu dobije obaveštenje o predstojećoj suši na mobilni telefon, ili kad lekar u ruralnoj ambulanti konsultuje kolegu iz glavnog grada putem telemedicine – tada tehnologija postaje društvena snaga.

Pandemija COVID-19 jasno je pokazala razliku između društava sa razvijenim IT kapacitetima i onih koja ih nemaju. Zemlje koje su imale jaku digitalnu infrastrukturu i razvijene e-usluge mogle su brže da pređu na rad od kuće, online nastavu i digitalno praćenje zdravstvenih podataka. McKinsey u svojim izveštajima beleži da su te zemlje pretrpele manji pad BDP-a i brže se vratile na pretkrizne nivoe, dok su druge izgubile dragoceno vreme i resurse.

Paradoks produktivnosti i digitalni jaz

Tehnološki napredak nije automatski garant produktivnosti. Postoji tzv. „paradoks produktivnosti“ – pojava da uprkos ubrzanom tehnološkom razvoju, statistike ponekad pokazuju spor rast produktivnosti. Razlog? Potrebno je vreme da se organizacije prilagode, procesi optimizuju i da obučeni ljudi počnu da koriste nove mogućnosti. Gartner navodi da je samo 48% digitalnih inicijativa u preduzećima ispunilo ili premašilo očekivane poslovne rezultate, dok ostale nisu ostvarile planirane benefite, najčešće zbog nedostatka obuke i strategije.

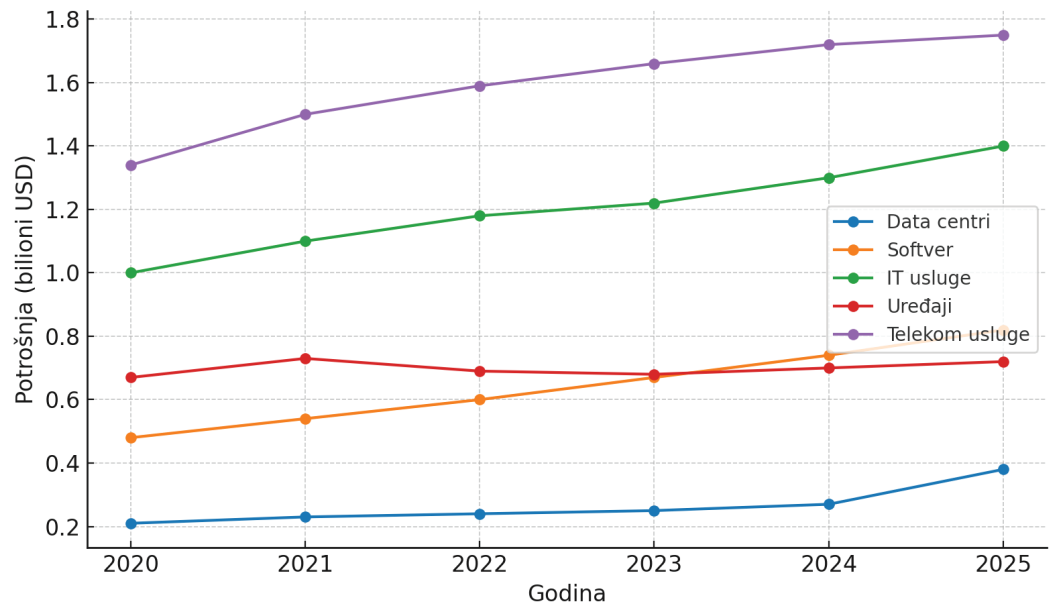
Digitalni jaz ostaje ozbiljan problem. Ako se investicije koncentrišu u

urbanim centrima, razlike između razvijenih i nerazvijenih regiona rastu. UN i Svetska banka upozoravaju da bez politika koje obezbeđuju ravnomeran pristup, tehnologija može da produbi postojeće društvene nejednakosti.

Budućnost: AI, IoT i inteligentne mreže

Sledeća decenija biće oblikovana kombinacijom veštačke inteligencije, Interneta stvari i – u nešto daljoj perspektivi – kvantnog računarstva. McKinsey Global Institute procenjuje da bi AI do 2030. mogao da generiše dodatnih 13-15 biliona dolara globalnog BDP-a. Međutim, ti dobici neće se ravnomerno raspodeliti – zemlje i kompanije koje prve razviju sposobnosti za implementaciju AI rešenja imaju značajnu prednost.

Na nivou preduzeća, *triple outperformers* – kompanije koje istovremeno ostvaruju rast prihoda, profitabilnost i dobre ESG rezultate – prema McKinsey-ju beleže 2-7 procentnih poena veću ukupnu stopu povrata akcionarima od konkurencije. U praksi, to znači da odgovorno investiranje, koje uključuje i društveni uticaj, donosi ne samo bolju reputaciju, već i direktnu finansijsku korist.



Rast globalne IT potrošnje 2020-2025 (Gartner) – segmenti: data centri, softver, usluge, uređaji...

Poslovne i društvene implikacije

Za kompanije, ulaganje u IT danas je pitanje opstanka, ne samo rasta. Klijenti i partneri očekuju brze, digitalno podržane procese, transparentne informacije i personalizovana iskustva. Države koje žele da privuku investicije moraju ponuditi ne samo poreske olakšice, već i digitalnu infrastrukturu i regulatorni okvir koji podržava inovacije.

Ulaganja u IT menjaju i samu strukturu rada. Automatizacija i AI preuzimaju rutinske zadatke, dok se ljudski rad pomera ka kreativnim, analitičkim i interpersonalnim veštinama. OECD upozorava da će obrazovni sistemi morati da se prilagode ovom trendu – škole i univerziteti treba da razvijaju digitalne i „meke“ veštine, kako bi radna snaga ostala konkurentna.

Ulaganje u budućnost

IT ulaganja su mnogo više od tehničkih projekata. Ona su strateški instrument društvenog razvoja. Zemlje i kompanije koje ih shvataju kao dugoročnu investiciju u ljude, procese i kulturu, a ne samo u opremu, beleže stabilniji rast, veću otpornost na krize i viši kvalitet života. Kao što pokazuje priča sa početka – jedan optički kabl može da poveže mnogo više od dva računara. Može da poveže ljude, ideje i budućnost.

Global Connectivity Index, koji meri povezanost infrastrukture i digitalne spremnosti zemalja, pokazuje da svaki dolar uložen u IKT infrastrukturu u proseku donosi 5 dolara povrata. Ulaganje u IT nije trošak, već multiplikator ekonomskog rasta

Cisco bezbednosna arhitektura kao ključ kontinuiteta i sigurnosti poslovanja kompanija

Kompanija Cisco, kao jedan od globalnih lidera u oblasti mrežnih i bezbednosnih rešenja, već decenijama gradi arhitekture koje imaju za cilj da kompanijama obezbede stabilnost i otpornost na napade. Upravo ideja da poslovanje danas zavisi od brzine i otpornosti u kriznim situacijama stoji iza Cisco bezbednosne arhitekture

 Nikola Milovanović, Technical Presales Architect

Danas je gotovo nemoguće zamisliti uspešan biznis bez snažne i pametno postavljene bezbednosne mrežne arhitekture. Pretnje su sve raznovrsnije – od sofisticiranih sajbernapada (npr. *spear phishing* i ransomware) do krađe podataka – a kompanije žive u okruženju gde je poslovni kontinuitet jednako važan kao i sam proizvod ili usluga koju nude. Gubitak podataka danas ne znači samo tehnički problem, već vrlo često gubitak poverenja partnera i klijenata, što u mnogim slučajevima može predstavljati nepovratan udarac za samu kompaniju.

Kompanija Cisco, kao jedan od globalnih lidera u oblasti mrežnih i bezbednosnih rešenja, već decenijama gradi arhitekture koje imaju za cilj da kompanijama obezbede stabilnost i otpornost na napade. Važnost takvih rešenja najbolje se vidi kroz realne događaje – podsetimo se samo tragedije rušenja Svetskog trgovinskog centra u Njujorku 2001. godine, kada su mnoge kompanije koje nisu imale adekvatno rešeno čuvanje i zaštitu podataka jednostavno prestale da postoje, dok su one koje su imale dobro osmišljene planove kontinuiteta poslovanja nastavile rad već posle nekoliko dana.

Fazna implementacija Cisco bezbednosne mrežne arhitekture predstavlja optimalno rešenje za većinu kompanija, jer omogućava da se kompleksni projekti sprovedu postupno, u skladu sa finansijskim planovima i prioritetima

Napadači vrebaju...

U našem okruženju, na brdovitom Balkanu, do pre pet ili šest godina problem kontinuiteta rada poslovnih IT sistema kompanija bio je uglavnom povezan s dostupnošću napajanja i pouzdanošću rada samih mrežnih uređaja, radnih stanica i servera. Danas, hteli mi to da priznamo ili ne, kompanije i organizacije u Srbiji se sve više suočavaju s problemima koji postoje u ekonomski najrazvijenijim državama sveta, a koji se odnose na sajbernapade. Broj sajbernapada u Srbiji je u stalnom porastu, napadi su sve sofisticiraniji (na primer, broj detekcija *ransomware*-a porastao je za 71,6 odsto u 2024. godini, dok je broj napada na banke i POS terminale šest puta povećan u odnosu na prethodnu godinu), očigledan je nedostatak

kadrova u sektoru sajberbezbednosti i nedovoljna je implementacija industrijskih bezbednosnih standarda.

Upravo ta lekcija – da poslovanje danas zavisi od brzine i otpornosti u kriznim situacijama – stoji i iza Cisco bezbednosne arhitekture, koja kombinuje savremene tehnologije i inteligentno upravljanje rizicima u jedinstveno rešenje.

Cisco bezbednosna arhitektura (*Cisco Security Architecture*) daje pregled Cisco bezbednosnog portfolija, najčešćih scenarija primene i preporučenih mogućnosti u okviru jedinstvene arhitekture. Ovaj referentni model povezuje se i sa oblastima koje prate industrijske bezbednosne okvire, kao što su NIST, CISA i DISA.

Osnovne komponente

Pet osnovnih komponenti Cisco bezbednosne referentne arhitekture su:

- lokalne mreže (*on-premises*) i mreže na ivici oblaka (*cloud edge*);
- bezbednost korisnika/zaposlenih i uređaja koje koriste;
- bezbednost opterećenja radnih stanica i aplikacija;





- centar za bezbednosne operacije, tzv. SOC (Security Operations Center) i
- bezbednost platformi u oblaku (cloud security).

▲
Cisco Security Platform

▼
Duo



uvodi mogućnost stalnog usklađivanja sa uvek prisutnim promenama u okruženju sajberbezbednosti.

Cisco koktel

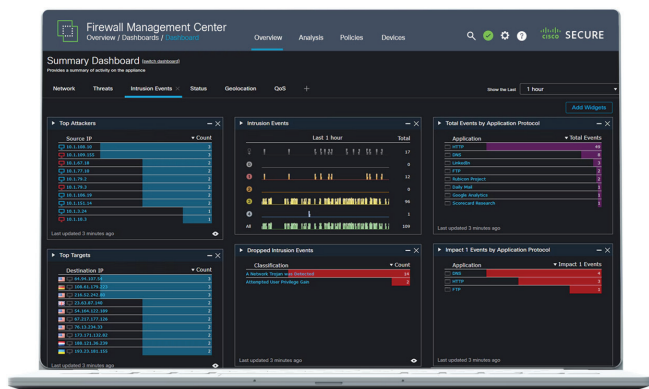
Nakon sagledavanja opštih aspekata, vreme je da pređemo na detaljnije predstavljanje sastojaka Cisco bezbednosnog „koktela“ koji kompanija omogućava kontinuitet i bezbednost poslovanja, odnosno miran san i nesmetan rad.

Cisco bezbednosna arhitektura sastoji se od funkcionalnih modula i mogućnosti koje pružaju višeslojnu zaštitu, kao što su Zero Trust (nulto poverenje za svakog korisnika), SASE (siguran pristup kao servis na ivici mreže) i XDR (prošireno otkrivanje i reagovanje za zaštitu uređaja koje koriste

Svaka kompanija ima jedinstveno mrežno okruženje (i lokalno i u oblaku) zasnovano na sopstvenim poslovnim potrebama, tako da nije neophodno odmah primeniti kompletnu Cisco bezbednosnu arhitekturu, već je preporuka da se radi fazna implementacija. Iskustvo iz višedecenijske prakse na domaćem IT tržištu, pokazuje da je druga bitna komponenta uspešnog bezbednosnog „koktela“ da kompanijski IT i bezbednosni tim razmotri sve bitne parametre bezbednosti poslovnog sistema (kao što su kritične poslovne aplikacije, koji zaposleni ili spoljni saradnici udaljeno pristupaju važnim resursima kompanije) i da zajedno sa Cisco ekspertima zajedno mapiraju svoj put bezbednosti.

Fazna implementacija Cisco bezbednosne mrežne arhitekture predstavlja optimalno rešenje za većinu kompanija, jer omogućava da se kompleksni projekti sprovedu postupno, u skladu sa finansijskim planovima i prioritetima. Istovremeno, ovakav model

▼
FMC



zaposleni i drugi krajnji korisnici) za SOC centar. Krajnji spoljni sloj predstavlja platforma pod nazivom Security Cloud Control. Ova platforma u oblaku koristi AI/ML algoritme, otvorena je i proširiva i omogućava jedinstveno upravljanje procenom rizika za sve unutrašnje module arhitekture. Talos je sistem globalne bezbednosne inteligencije sa ciljem praćenja pretnji, pružanja akcionih informacija o pretnjama i istraživanje malvera u realnom vremenu, na celoj globalnoj Internet mreži. SOC funkcionalnosti, poput reputacije IP adresa i domena, SNORT potpisa, analize i kontrole malicioznih fajlova, kategorizacije URL-ova i AI odbrane, dostupne su u više tačaka korporativnog sistema – krajnji uređaji, firewall uređaji nove generacije (NGFW), e-mail, cloud gateway-i i radne stanice i serveri.

Firewall sledeće generacije

Cisco NGFW (Next-Generation Firewall) pruža naprednu zaštitu mreže kombinujući tradicionalni firewall sistem sa funkcijama kao što su inspekcija aplikacija, prevencija upada i integrisana zaštita od malvera. Omogućava kompanijama da precizno kontrolišu pristup aplikacijama i resursima, dok AI i analitika pomažu u prepoznavanju i blokiranju sofisticiranih pretnji.

Ispod sloja operacija bezbednosti nalaze se Zero Trust i SASE moduli, koji pokrivaju celu arhitekturu – od korisnika i uređaja do radnih opterećenja (radne stanice i serveri) i aplikacija u okruženju više oblaka (multicloud). Funkcionalnosti za bezbednost korisnika i uređaja osiguravaju što jednostavnije korisničko iskustvo kroz jedinstveni Secure Client, uz visoku zaštitu od pretnji poput phishing-a i ransomware-a. Put podataka od korisnika/uređaja do radnih stanica i servera, i aplikacija može se ostvariti preko Cloud Edge mreže ili lokalnih (on-premises) mrežnih modula.

Jedna od osnovnih prednosti sistemski razvijene arhitekture leži u mogućnostima deljenja kontekstualnih informacija i identiteta. Osnovna funkcionalnost počinje sa Cisco Identity Services Engine (ISE) i proteže se do Cloud Edge, SD-WAN, IoT i radnih opterećenja i aplikacija kako bi se delile informacije o bilo kojem uređaju koji pristupa zaštićenim resursima kompanije. S druge strane, omogućena je integracija s rešenjima trećih strana (drugih proizvođača), tako da postoji dinamička i detaljna kontrola pristupa korisnika i aplikacija.

Krađa identiteta danas čini većinu bezbednosnih propusta. Cisco Duo je rešenje za višefaktorsku autentifikaciju (MFA) koje kompanijama omogućava da zaštite pristup svojim aplikacijama i podacima. Korisnici (zaposleni i spoljni saradnici) potvrđuju svoj identitet putem mobilne aplikacije, SMS-a, poziva ili hardverskog tokena, čime se znatno smanjuje rizik od neovlašćenog pristupa. Duo prati ponašanje korisnika i uređaja, pružajući uvid u potencijalne pretnje

i sigurnosne propuste. Pored toga, lako se integriše s postojećim aplikacijama i servisima u oblaku, što olakšava primenu u svakoj kompaniji.

Zero Trust arhitektura

Cisco Identity Intelligence je ključni deo *Zero Trust* arhitekture i pruža uvid u ponašanje korisnika preko različitih izvora identiteta koji se obično nalaze u mrežama kompanije. Bezbednosna politika kompanije treba da bude jasno definisana i mora reagovati na promene zasnovane na različitim podacima, kao što su informacije o pretnjama, trendovi logovanja, neuobičajeno ponašanje pri prijavljivanju, nerealna putovanja i slično.

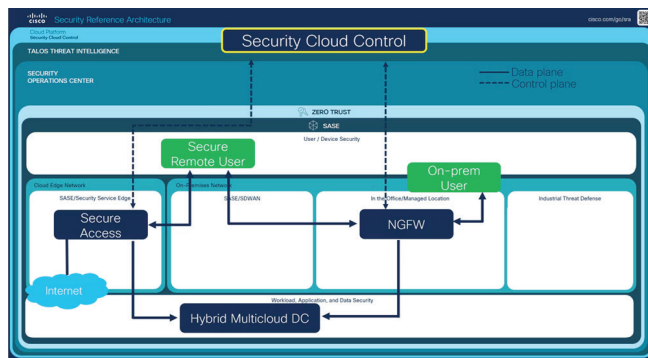
Zato referentna bezbednosna arhitektura omogućava primenu ovakvih politika, uključujući *Identity Threat Detection & Response (ITDR)*, kroz *cloud edge* i lokalne mreže, kao i radna opterećenja i aplikacije u *multicloud* okruženju, kako bi SOC analitičari mogli brzo da reaguju na incidente širom mreže.

Cilj platforme *Security Cloud Control* je da omogući ujednačavanje politika i deljenje zajedničkih objekata unutar nje, pružanje integrisane arhitekture, kao što je *Hybrid Mesh Firewall*, gde se *firewall* servisi na cloud edge, lokalnim mrežama i *multicloud data* centrima mogu ujediniti i pojednostaviti, smanjujući mogućnost ljudske greške.

Security Cloud Control koristi AI mogućnosti kako bi primenio zajedničku politiku (na primer: „Zabrani Petru da koristi finansijsku aplikaciju na mobilnom uređaju nakon 17 h“) na različitim tačkama primene – fizičkim, virtuelnim ili *cloud* sigurnosnim grupama – kroz celu *multicloud* mrežu.

Univerzalni ZTNA (pristup mreži sa nultom tolerancijom) koristi *Cisco Secure Client* i omogućava korisnicima i njihovim uređajima jednostavan i siguran pristup bilo kojoj aplikaciji, bez potrebe za aktiviranjem punog VPN-a ili razmišljanjem o tome kako bezbedno pristupiti željenoj aplikaciji.

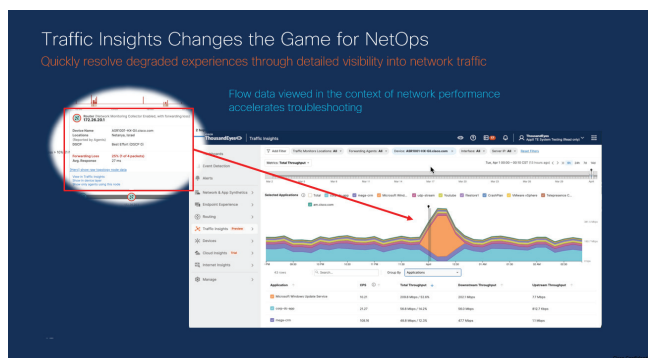
Cilj *Zero Trust* pristupa je da korisnicima bude dodeljen minimalan potreban nivo pristupa kako bi se



Universal ZTNA

sprečio neovlašćen ili prekomeran pristup. *Universal ZTNA* omogućava VPN po aplikaciji kada je moguće i definiše pravi put podataka u skladu s politikom aplikacije. Na primer, finansijska kompanija koja ne želi da koristi oblak (*cloud*), može povezivati korisnike s kritičnim aplikacijama preko lokalnih mreža, dok se nekritične aplikacije mogu koristiti preko *cloud edge* mreže.

Thousand Eyes v2



Procena performansi

Cisco ThousandEyes pruža detaljan uvid u performanse mreže, Interneta i servisa u oblaku, omogućavajući kompanijama da prate dostupnost i brzinu svojih aplikacija. Ovaj sistem detektuje probleme u realnom vremenu, od lokalnih mreža do globalnog Interneta,

i pomaže timovima da brzo identifikuju uzrok problema. *ThousandEyes* kombinuje merenja s vizuelizacijom podataka, čineći složene mrežne performanse jednostavnijim za praćenje i razumevanje. *Cisco AppDynamics* je platforma za praćenje performansi aplikacija, a omogućava identifikaciju i rešavanje problema pre nego što utiču na krajnje korisnike, optimizujući performanse i stabilnost sistema. *AppDynamics* prati sve slojeve aplikacije, od baze podataka do korisničkog interfejsa, i povezuje metrike s poslovnim rezultatima. Korišćenjem navedena dva *Cisco* sistema, koji nude vizuelizaciju i detaljne analize, timovi za IT i razvoj kompanije mogu brže donositi odluke i poboljšati efikasnost poslovnih procesa.

Danas nijedna kompanija ne može da zanemari sajberbezbednost – gubitak podataka znači gubitak poverenja i često ozbiljne poslovne posledice. *Cisco* bezbednosna arhitektura pokazuje kako se modernim alatima, kao što su *Security Cloud Control*, *Universal ZTNA* i *Identity Intelligence*, može obezbediti višeslojna zaštita i inteligentno upravljanje pristupom korporativnoj mreži. Kroz integrisane module i AI podršku, kompanije mogu da pojednostave bezbednosne politike, smanje ljudske greške i brzo reaguju na pretnje. Ukratko, *Cisco* je ponudio bezbednosnu arhitekturu sa svim potrebnim sistemima koja predstavlja most između bezbednog IT okruženja i kontinuiteta poslovanja, čineći mreže otpornijim i korisničko iskustvo jednostavnijim.

comtradedistribution.com

Cisco je ponudio bezbednosnu arhitekturu sa svim potrebnim sistemima koja predstavlja most između bezbednog IT okruženja i kontinuiteta poslovanja



Cisco Secure Wins

Synology Enterprise NAS serije i High Availability

Kompanije se suočavaju sa sve većim izazovima u upravljanju i zaštiti podataka. Brz pristup, sigurnost i fleksibilnost postali su ključni faktori za održavanje konkurentnosti. Synology nudi moćna rešenja koja direktno odgovaraju na ove izazove, posebno kroz enterprise NAS serije i Synology High Availability

Za organizacije koje imaju visoke zahteve u pogledu performansi i dostupnosti podataka, Synology enterprise NAS uređaji donose kombinaciju skalabilnosti, sigurnosti i jednostavnog upravljanja. Serije kao što su FS, SA, UC i HD omogućavaju:

- Skalabilnost bez kompromisa – lako prilagođavanje rastućim potrebama kompanije.
- Pouzdane performanse – stabilan rad čak i kod intenzivnih radnih opterećenja.
- Sigurnost podataka – napredne opcije zaštite i brze oporavke u slučaju incidenta.

Synology High Availability

Za svaku organizaciju koja ne može da dozvoli prekid u radu sistema,

Synology će s ponosom učestvovati na predstojećoj Tech Hosted konferenciji, zajedno s vodećim enterprise vendorima



Synology High Availability obezbeđuje automatski prelazak s primarnog na sekundarni server. Ukoliko primarni server iz bilo kog razloga prestane da radi, sekundarni odmah preuzima ulogu u realnom vremenu – bez zastoja u radu i bez gubitka podataka.

Ključne prednosti uključuju:

- Maksimalnu dostupnost servisa – poslovne aplikacije i fajlovi uvek dostupni korisnicima.

Menadžeri dobijaju sigurnost da njihovi timovi mogu raditi neometano, dok istovremeno smanjuju operativne rizike i optimizuju troškove

- Zaštitu od gubitaka i incidenata – eliminiše rizik od prekida rada zbog hardverskih kvarova.
- Neprimetan prelazak – zaposleni nastavljaju s radom bez prekida produktivnosti.
- Jednostavno upravljanje – centralizovani sistem za nadzor i kontrolu.

Synology na Tech Hosted konferenciji

Synology će s ponosom učestvovati na predstojećoj Tech Hosted konferenciji, zajedno s vodećim enterprise vendorima, kao što su Dell, HPE i Fortinet. Na konferenciji će predstaviti novosti i rešenja čije je lansiranje zakazano u narednom periodu.

Pozivamo vas da nam se pridružite i otkrijete na koji način Synology može postati pouzdan partner u digitalnoj transformaciji vašeg biznisa. Synology kombinacijom enterprise NAS uređaja i High Availability funkcionalnosti donosi kompanijama sigurnost, stabilnost i kontrolu nad ključnim poslovnim procesima. Na taj način menadžeri dobijaju sigurnost da njihovi timovi mogu raditi neometano, dok istovremeno smanjuju operativne rizike i optimizuju troškove.

sy.to/j3ozy



Brz oporavak poslovnog sistema i posle najtežih kibernetapada

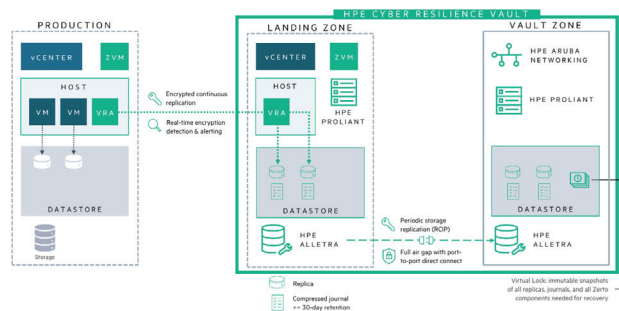
Sve je jasnije da se ransomware i hakerskim napadima jako teško odupreti, stoga treba ozbiljno razmišljati o brzom oporavku posle eventualnog napada. HPE Cyber Resilience Vault omogućava brz oporavak poslovanja uz najviši nivo zaštite podataka

Pretnje od *ransomware* i drugih kibernetapada nastavljaju da rastu, kako po učestalosti tako i u tehnikama i sofistikaciji. Napadi postaju sve jeftiniji otkako su se pojavile kriminalne mreže koje nude *ransomware* napade kao uslugu, a uspešne ucene motivišu i finansiraju razvoj sve novijih *malware* programa.

Da bi se nosile u koštac sa ovakvim izazovima, kompanije sve više ulažu u razne tehnologije zaštite, u pokušaju da preduprede upad i umanje načinjenu štetu. Apsolutnu zaštitu je nemoguće garantovati, pa su od jednake važnosti i tehnologije oporavka. To su rešenja koja omogućavaju da se posle napada poslovanje oporavi i nastavi sa ispravnim podacima, makar i s nekim gubitkom vremena.

HPE Cyber Resilience Vault nudi najviši nivo zaštite podataka, uz veoma brz oporavak (nizak RTO). Čak i ako je sva oprema u produkcionom računskom centru ispravna, povraćaj velike količine podataka sa *backup* uređaja niskih performansi može produžiti oporavak za više dana ili čak sedmica. Pretraga i utvrđivanje koja verzija *backup*-a nije inficirana dodatno produžava proces.

Ukoliko zakonodavni organi ili interna služba bezbednosti vrše uviđaj na produkcionoj opremi, može biti neophodno da se poslovne aplikacije privremeno izvršavaju na odvojenoj lokaciji – što nije nešto što namenski



▲
HPE Cyber Resilience Vault u potpuno virtualiziranom okruženju

backup uređaji ili arhivski *storage* u *cloud*-u omogućavaju. Imperativ je što pre nastaviti s poslovanjem, što tradicionalna *backup* i arhivska rešenja ne omogućavaju, jer nisu ni dizajnirana s takvim ciljem na umu.

HPE Cyber Resilience Vault

HPE Cyber Resilience Vault je rešenje dizajnirano da odgovori ovakvim izazovima, zasnovano na HPE Alletra *storage*-u, HPE ProLiant serverima, HPE Aruba mreži i HPE Zerto softveru. Predstavlja integrisan sistem za zaštitu podataka uz primenu svih najviših standarda zaštite, i s tri osnove:

Replikacija i detekcija – stalna kvazisinhrona replikacija podataka štiti svaki upis u realnom vremenu, istovremeno detektujući bilo kakve anomalije, o kojima obaveštava nadzorni sistem.



ŠTA JE HPE ZERTO?

HPE Zerto je softversko rešenje za oporavak od otkaza (*disaster recovery*), uz kontinuiranu zaštitu podataka (CDP). U trenutku kada se pokrene, HPE Zerto će iskopirati virtuelnu mašinu na lokaciju koju odredi korisnik. U HPE Cyber Resilience Vault-u, to je *Landing* zona. Od trenutka kada se mašina iskopira, HPE Zerto će nastaviti da je „prati“ u produkcijskom okruženju i svakih nekoliko sekundi beleži njihove upise u žurnal transakcija.

U žurnalu će ostati zabeležene inkrementalne promene mašine na svakih nekoliko sekundi, a maksimalno u trajanju do 30 dana. To omogućava da u

slučaju bilo koje vrste otkaza virtuelne mašine vratimo celu virtuelnu mašinu ili samo pojedinačne fajlove na bilo koje izabrano stanje iz žurnala.

Zerto nudi mogućnost testiranja *disaster recovery* plana. U tom slučaju, HPE Zerto će podići virtuelne mašine na lokaciji koju korisnik odredi, uz mogućnost da se to uradi uz promenu mrežnih parametara tih mašina. Ova operacija je izuzetno brza – za virtuelne mašine srednje veličine (stotinak gigabajta) ona traje svega nekoliko desetina sekundi. Upravo po ovoj osobini, softver je i dobio ime: Zerto dolazi od Zero RTO (*Recovery Time Objective*).

Izolacija i bezbednost – izdvojena Vault zona je *offline*, mrežno izdvojena i čuva nepromenljive kopije na bezbednom HPE hardveru visokih performansi.

Testiranje i oporavak – jednostavno identifikujte tačke za oporavak pre infekcije i potom brzo oporavite aplikacije sačinjene od višestrukih VM, čak i u okruženjima sa hiljadama VM.

Kako HPE Cyber Resilience Vault radi?

Landing zona je uparena s produkcionim okruženjem, bazirana na VMware vSphere i može predstavljati tradicionalni DR ako je locirana na izdvojenoj lokaciji. Na *Landing* zonu se pomoću HPE Zerto softvera kontinuirano i kvazisinhrono repliciraju zaštićene VM s produkcionog okruženja. HPE Zerto CDP replicacija nema nikakve agente, tako da ne postoji mogućnost da *malware* zaobiđe ili isključi HPE Zerto zaštitu unutar VM. Svaki upis sa štice VM se kompresuje, enkriptuje i prenosi u *Landing* zonu. Tu se upisuje u CDP žurnal – tekući zapis sa stotinama ili hiljadama *restore* tačaka, s konzistencijom između različitih VM i sačuvanim redosledom upisa (*write-order fidelity*). Žurnal čuva od jednog sata do 30 dana podataka i predstavlja prvu i najbolju opciju za oporavak kod *ransomware* napada.

Vault zona je fizički kolocirana s *Landing* zonom, fizički izolovana (*Clean room* – čista soba), bez aktivnih mrežnih konekcija (*air-gap*) i nema pristupa ni Internetu ni

produkcionim mrežama. Pošto nema centralne upravljačke ravni, *Vault* zona nema izložene ni *management* portove i nema nijednu tačku kompromisa. HPE *Alletra* u *Landing* zoni i *Vault* zoni koriste direktno povezane IP portove za *Remote copy over IP* (RCIP) replicaciju. Repliciraju se svi podaci iz *Landing* zone, uključujući HPE *Zerto* žurnale i replike. Ovaj pristup kombinuje najbolje aspekte sinhrono replicacije (hiperniski RPO i visoke performanse) i tradicionalne asinhrono replicacije: veća dopuštena latencija, bez uticaja na performanse produkcije, i sa smanjenim zauzećem *storage*-a.

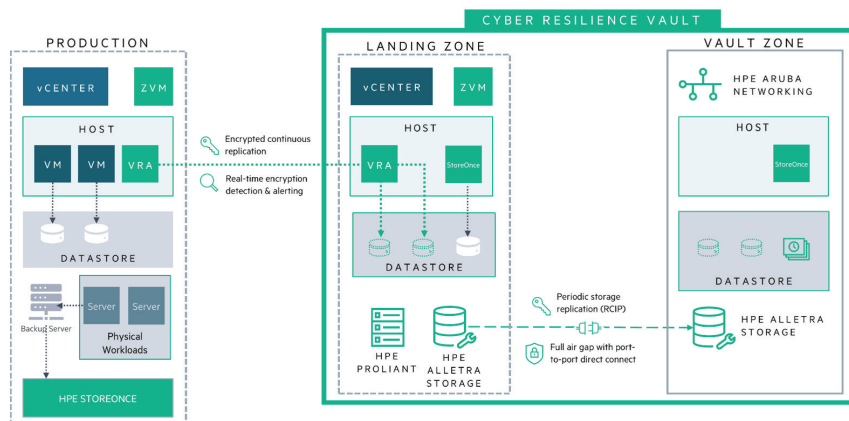
Proces oporavka

Proces oporavka je predviđen za različite scenarije infekcije, uključujući sledeće:

Zaraza pojedinih fajlova / direktorijuma / VM: ako je zona udara *ransomware*-a ograničena na pojedine fajlove i direktorijume unutar VM, pogođeni resursi se mogu gotovo trenutno oporaviti iz HPE *Zerto* žurnala na stanje iz 5-15 sekundi pre infekcije.

Ako je više VM zaraženo, HPE *Zerto* ih može skoro trenutno oporaviti u produkcijsko okruženje bez međukoraka poput *Storage vMotion*-a.

Zaraza celokupne produkcije: ukoliko su sve VM na produkcionoj/ primarnoj lokaciji inficirane, ali *Landing* zona nije, kompletan *failover* omogućava da se produkcija restartuje u vremenu merenom minutima.



RPO I RTO?

RPO i RTO su dva osnovna parametra koja opisuju očekivanja za koja je dizajniran sistem zaštite podataka, što je najčešće *backup* sistem.

Recovery Point Objective – RPO je parametar koji procenjuje koliki je najveći gubitak podataka, mereno vremenski. Ukoliko se *backup* nekog sistema vrši svakog dana, onda je njegov RPO 24 časa. Skraćivanje RPO-a se postiže češćim *backup*-om, što obično ima negativan uticaj na performanse produkcionih sistema.

Recovery Time Objective – RTO je parametar koji procenjuje koliko je vremena potrebno da se sistem oporavi iz zaštitnih kopija posle katastrofe. RTO je teško proceniti unapred, jer veoma zavisi od obima nastale štete, performansi sistema na kojima se čuvaju zaštitne kopije, stanja i performansi primarnih *storage*-a i slično. U manje katastrofalnim situacijama, RTO se obično kreće u opsegu od nekoliko sati do nekoliko dana.

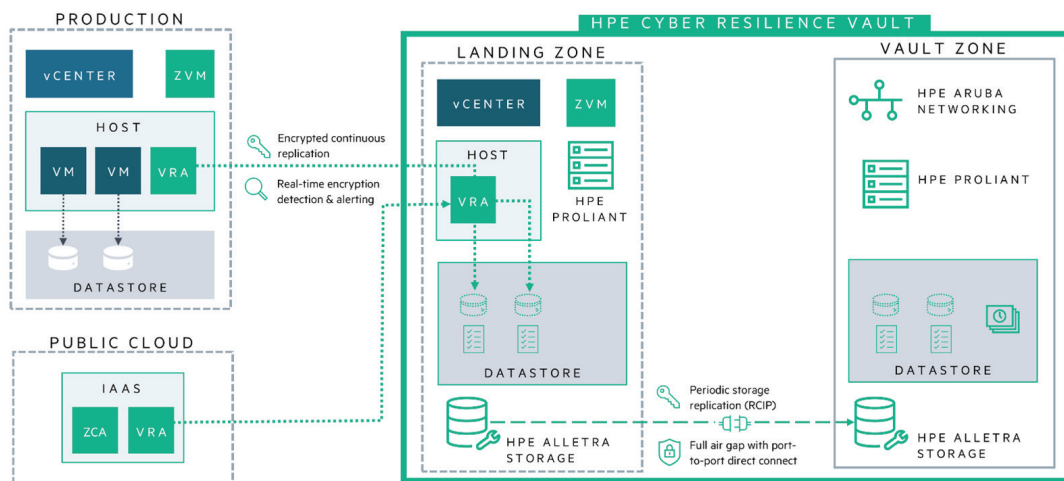
HPE *Alletra* je all-NVMe *storage* visokih performansi i visoke pouzdanosti i omogućava da se produkcija na *Landing* zoni izvršava bez gubitka performansi i potrebe za dodatnim sekundarnim *storage*-om.

Apsolutnu zaštitu od ransomware napada je nemoguće garantovati, pa su veoma važne i tehnologije oporavka, rešenja koja omogućavaju da se poslovanje u najkraćem roku oporavi

Zaraza više lokacija: ako se dogodi da su i produkciona i sekundarna lokacija zaražene (recimo, enkriptovani hostovi i brzo širenje infekcije uprkos mrežnoj segmentaciji), HPE *Cyber Resilience Vault* postaje najbezbednija čista soba u kojoj se radi oporavak. Evo kratkog sižea procesa oporavka:

- Ponovo napraviti lokaciju za oporavak: unutar *Vault* zone iskoristiti *immutable snapshot* da bi se oporavili VMFS i sačuvali UUID potpisi resursa.
- Oporaviti HPE *Zerto*: pošto je HPE *Zerto* visoko otporan i automatizovan, virtuelni menadžeri i *data mover*-i će se vratiti *online* i nastaviti rad bez ručne rekonfiguracije ili *setup*-a.
- Oporaviti podatke: koristeći HPE *Zerto* žurnale, odaberite jedan od hiljada dostupnih trenutaka za

◀ **Zaštita fizičkih servera putem standardnog backup i HPE StoreOnce**



oporavak da biste podigli sve VM u proizvoljnom redosledu. Orkestracija koja je deo HPE Zerto i visoke performanse HPE Alletra storage-a daju RTO u minutima i satima, umesto danima i nedeljama. Aplikacije sastavljene od više VM se brzo oporavljaju iz snimka u istom vremenskom trenutku, minimizujući potrebu za ručnom rekonfiguracijom posle oporavka.

Zaštita kompleksnih okruženja

Premda je zaštita VM pomoću HPE Zerto svakako tehnološki najnapredniji aspekt, arhitekta HPE Cyber Resilience Vault-a nisu zaboravili ni zaštitu složenih okruženja.

Za okruženja s kritičnim servisima na fizičkim serverima, omogućena je replikacija podataka iz backup-a putem HPE StoreOnce. Sam softver za backup mora da podržava HPE StoreOnce kao backup uređaj, koji će automatski preneti podatke u virtualni server u Landing zoni.

I tu se fleksibilnost ne završava – postojanje HPE Zerto Cloud Appliance-a omogućava zaštitu podataka iz

Ako je zona udara ransomware-a ograničena na pojedine fajlove i direktorijume unutar VM, pogođeni resursi se mogu gotovo trenutno oporaviti iz HPE Zerto žurnala na stanje iz 5-15 sekundi pre infekcije

javnog cloud okruženja u vašem HPE Cyber Resilience Vault-u.

HPE Zerto Cloud Appliance je dostupan u većini vodećih javnih cloud provajdera, kao što su Amazon, Google, Microsoft, Oracle ili IBM.

Projektovan za bezbednost i performanse

HPE Cyber Resilience Vault u sebi objedinjuje vrhunsku bezbednost i najviše performanse, ispunjavajući i najstrože standarde, nudeći:

- potpuni air gap sa izolovanim Vault-om,

Zaštita hibridnog cloud okruženja



ALI JA IMAM OPREMU RAZLIČITIH PROIZVOĐAČA!

HPE Zerto je potpuno nezavisan od hardvera na kome se izvršava. Najvažniji zahtevi su da je štićeno okruženje virtualizirano, i da je virtualizacija izvršena na jednoj od podržanih platformi: VMware vSphere ili HyperV.

Uskoro će se ovoj listi virtualizacionih platformi pridružiti i HPE Morpheus VM Essentials – najnovija alternativa na tržištu. Fizički (ne-virtualizovani) serveri se mogu štititi pomoću HPE StoreOnce koji replicira standardne backup-e podataka.

Uz HPE Cyber Resilience Vault sada je dostupno rešenje najviše bezbednosti i performansi, koje će se suprotstaviti pretnji ransomware-a

- Zero Trust arhitekturu,
- ojačane aplikativne VM bazirane na Linux-u,
- decentralizovano upravljanje bez jedinstvene tačke za kompromitaciju,
- nepromenljive offsite i offline kopije podataka,
- zaštićeni Tamper-proof NTP,
- detekciju enkripcije podataka u realnom vremenu,
- proširivost na 10.000+ VM po vCentru,
- All-NVMe storage najnovije generacije za privremeno izvršavanje bilo koje aplikacije pri oporavku,
- storage sa garancijom 100% dostupnosti u Landing zoni,
- sav hardver zaštićen Silicon Root Of Trust bezbednosnim procesorima.

Stvarna kiberotpornost

Uz HPE Cyber Resilience Vault sada je dostupno rešenje najviše bezbednosti i performansi da se suprotstavi pretnji ransomware-a. Jedinstvena decentralizovana arhitektura HPE Zerto omogućava brz oporavak u air-gap okruženju čak i posle najtežih napada.

- Drastično smanjen downtime nakon napada.
- Izbegava se direktan ili indirektan gubitak prihoda.
- Pomaže pri dostizanju regulatornih zahteva poput HIPAA, DORA, GDPR, SOX, ili FISMA/ NIST SP 800-34.

Sva kompleksnost sakrivena iza jedinstvenog rešenja od jednog vendara i s najboljim proizvodima u svakom koraku oporavka posle kibernetičkog napada.

Za upite u vezi sa HPE rešenjima za disaster recovery i ransomware zaštitu obratite se našem lokalnom stručnjaku Milanu Avramoviću na m.avramovic@selectium.com.

 hpe.com



bizit.rs

Dvanaesta BIZIT konferencija

REŠENJA, NE IZGOVORI

4. i 5. novembar 2025. • Hotel Metropol, Beograd



Upoznajte lidere iz sveta IT-ja, digitalne infrastrukture i biznisa.
Otkrijte praktična rešenja za realne poslovne izazove.

PRIJAVITE SE



AI • CLOUD • DATA CENTRI • ICT BEZBEDNOST • BIZNIS INOVACIJE • POSLOVNI SOFTVER

Elektronsko bolovanje

Kada je digitalizacija zdravstva tek počinjala da puzi, malo ko je mogao da zamisli dan kada će pacijent moći da ostane u krevetu, a da lekar, poslodavac i zdravstveni fond već znaju da je na bolovanju... i to bez ijednog papira. Taj dan je došao i Srbija je u martu 2025. konačno uvela sistem elektronskog bolovanja

■ Nenad Cvjetićanin

Nova usluga e-bolovanje objedinjuje informacione sisteme koje koriste lekari, poslodavci i Republički fond za zdravstveno osiguranje (RFZO), omogućavajući da se elektronske doznake šalju direktno iz lekarske ordinacije ka poslodavcu i Fondu, bez potrebe da zaposleni lično odnosi dokumentaciju i to putem portala eUprava.

Bez jurenja papira

Uvođenje e-bolovanja nije samo još jedan administrativni *upgrade*, već korak koji menja suštinu odnosa građanina i države. U trenutku kada je bolestan i ranjiv, zaposleni više neće morati da juri pečate, redove i kopije – sistem prepoznaje njegov status i sve relevantne strane dobijaju pravovremene informacije. Poslodavac zna kada zaposleni nije na poslu, RFZO zna kada i koliko dugo traje bolovanje, a pacijent ima mogućnost da se fokusira na ono što je najvažnije – da ozdravi.

Važan aspekt nove usluge leži i u njenom potencijalu da smanji zloupotrebe. Nije tajna da su pojedini poslodavci i strani investitori godinama izražavali zabrinutost zbog, kako tvrde, prekomernog korišćenja bolovanja. Statistički podaci ukazuju da čak 20 odsto zaposlenih u proseku nije na poslu, pri čemu deo tih bolovanja nema zakoniti osnov, odnosno predstavlja zloupotrebu bolovanja.

Kod odsustava preko 30 dana, sistem automatski generiše uput za lekarsku komisiju Republičkog fonda za zdravstveno osiguranje (RFZO), a kompletna dokumentacija se šalje elektronski



Kroz elektronsko bolovanje, moguće je brže i preciznije kontrolisati osnovanost doznaka, trajanje bolovanja i upariti ih s podacima iz zdravstvenog sistema. Digitalni trag ne samo da ubrzava obradu već i omogućava retroaktivnu analizu i reagovanje u realnom vremenu.

U prvoj fazi primene, elektronsko bolovanje uvedeno je u četiri beogradska doma zdravlja: na Voždovcu, Vračaru, u Zemunu i Obrenovcu. Već u prvih desetak dana izdato je oko 1.400 e-bolovanja. Lekari sada, odmah nakon pregleda, elektronski unose sve relevantne podatke u informacioni sistem zdravstvene ustanove. Potvrda o privremenoj

sprečenosti za rad automatski se prosleđuje portalu e-Zdravlje, gde je dostupna pacijentu i, u punoj fazi implementacije, i poslodavcu.

Za pacijente koji su registrovani na portalu e-Zdravlje, potvrda o bolovanju stiže elektronskim putem, dok oni koji nisu deo sistema i dalje mogu dobiti papirnu verziju – odmah u ordinaciji. Obaveza zaposlenog ostaje ista: da u roku od tri radna dana, od dana otvaranja bolovanja, obavesti poslodavca. Ali, ono što se menja jeste to da više nema potrebe za fizičkim prenošenjem dokumentacije. Digitalni zapis, jednom unesen, postaje dostupan svima kojima je potreban – lekarskoj

komisiji, Fondu, poslodavcu i pacijentu.

Lakše i lekarima

Procedura je dodatno olakšana i za lekare. Ako pacijent ne dođe na zakazanu kontrolu, a prethodno se nije javio, sistem automatski zatvara bolovanje i generiše odgovarajuće doznake. U slučaju da se simptomi nastave, lekar može na licu mesta produžiti bolovanje, uz elektronski unos novog datuma kontrole. Kod dužih odsustava – preko 30 dana – sistem automatski generiše uput za lekarsku komisiju Republičkog fonda za zdravstveno osiguranje (RFZO), a kompletna dokumentacija se šalje elektronski.

Ovaj projekat sprovodi Ministarstvo zdravlja u saradnji sa RFZO i Kancelarijom za IT i eUpravu, dok podršku pruža Nacionalna alijansa za lokalni ekonomski razvoj (NALED). Ova inicijativa direktno odgovara na preporuke iz Sive knjige – strateškog dokumenta koji sadrži ključne zahteve i sugestije privrede za unapređenje poslovnog ambijenta u Srbiji.

Građani nisu u obavezi da koriste digitalnu formu – potvrde se i dalje mogu štampati u ordinaciji za sve koji nisu deo e-Zdravlje sistema. Iako je predviđeno da e-bolovanje funkcioniše bez papira, i dalje postoje situacije u kojima je fizičko prisustvo potrebno. Na primer, kada pacijent nije registrovan na portalu e-Zdrav-

lje, kada je neophodna kontrola kod lekara zbog medicinskog stanja ili kada poslodavac još nije uključen u sistem. Upravo zato, uspeh ove reforme ne zavisi samo od zdravstvenih ustanova već i od angažovanja poslodavaca i same privrede. U širem kontekstu, e-bolovanje predstavlja deo nacionalne strategije digitalizaci-



Kroz elektronsko bolovanje moguće je brže i preciznije kontrolisati osnovanost doznaka, trajanje bolovanja i upariti ih s podacima iz zdravstvenog sistema

Građani nisu u obavezi da koriste digitalnu formu – potvrde se i dalje mogu štampati u ordinaciji za sve koji nisu deo e-Zdravlje sistema

je zdravstvenog sistema. Ministarstvo zdravlja je već usvojilo pravilnik o primeni elektronskog zdravstvenog kartona (eKartona), a u planu je i njegovo potpuno uvođenje.

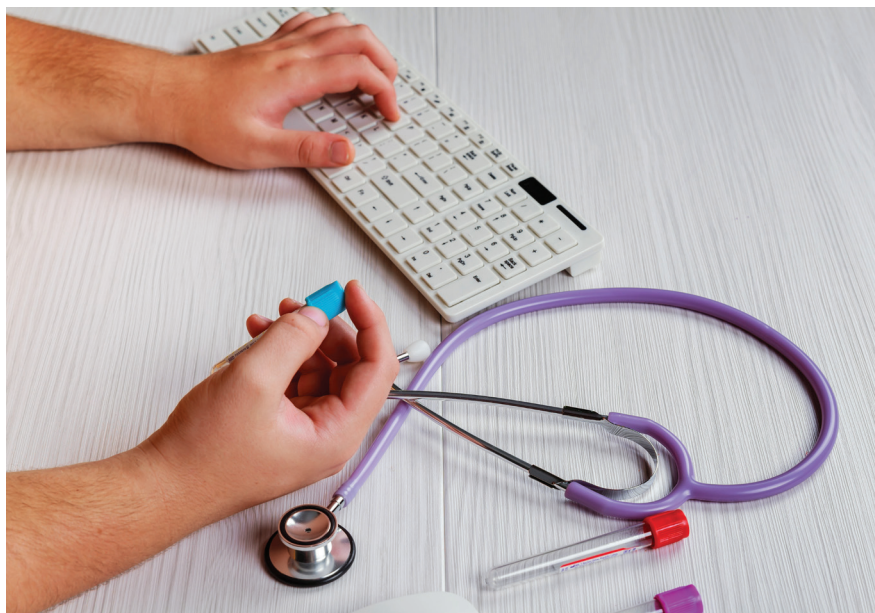
Držimo korak

Zanimljivo je da Srbija u ovom domenu ne zaostaje za regionom, na protiv. Hrvatska je, primera radi, već implementirala sistem e-doznaka, gde lekari elektronski šalju potvrde o bolovanju direktno HZZO-u i poslodavcu već nekoliko godina. Tamošnje vlasti otišle su i korak dalje, uvevši strože kontrole – u 2024. godini čak 26 odsto bolovanja je zatvoreno kao neosnovano. Uz to, hrvatski zakon predviđa kazne i za pacijente i za lekare zbog neosnovanih bolovanja, a planirano je i povećanje maksimalnih naknada kako bi sistem bio pravedniji i stimulativniji. Slovenija i Mađarska takođe primenjuju elektronske elemente u upravljanju bolovanjem, ali često u kombinaciji s papirnim dokumentima, što čini Hrvatsku i Srbiju liderima u regionu kada je reč o potpunoj digitalizaciji ovog segmenta zdravstvene administracije.

Nijedan sistem, pa ni digitalni, nije savršen. Da bi e-bolovanje zaista funkcionisalo, moraće da se obezbedi pravna sigurnost, zaštita podataka o ličnosti pacijenata (podaci o bolesti predstavljaju naročito osetljive podatke), tehnička stabilnost sistema, kao i puna obuka za lekare i administratore. Digitalizacija zdravstva i javne uprave često je opterećena nepoverenjem, administrativnim zastojećima i tehničkim izazovima. Ipak, iskustvo pokazuje da kada građani osete koristi – manje čekanja, manje šaltera, više sigurnosti – digitalne usluge postaju prirodan izbor. E-bolovanje je upravo takva usluga: lako razumljiva, opipljivo korisna i simbolično važna.

U svetu gde je vreme dragoceno, ovakvi iskoraci predstavljaju ne samo tehnološki napredak već i znak da država i privreda mogu biti brže i efikasnije.

Advokat Nenad Cvjetičanin je rukovodeći partner u kancelariji Cvjetičanin&partneri



Moda i tehnologija

Moda i tehnologija na prvi pogled deluju kao dva sveta koja retko imaju dodirnih tačaka. Ali upravo u njihovom spoju leži snaga modernog retail biznisa. Kada iza kulisa modne imperije, kakva je Fashion Company koja posluje na osam regionalnih tržišta, stoji snažan IT sektor, rezultati nisu samo vidljivi – oni su temelj uspeha

Dejan Ristanović

Jedan od onih koji svakodnevno gradi IT temelje modne industrije je Dušan Brdar, direktor IT sektora Fashion Company, jednog od vodećih modnih sistema u regionu koji okuplja više od 80 svetskih brendova u okviru svoja tri najveća *multibrend* koncepta: *Fashion&Friends*, *XYZ* i *Shoezen*. Najpoznatiji među njima su *Diesel*, *Tommy Hilfiger*, *BOSS*, *Calvin Klein*, *Replay*, *HUGO*, *Guess*, *Steve Madden*...

Karijeru je započeo kao *Business Systems Analyst*, a tokom vremena, profilisao se kao ključni tehnološki strateg u svetu mode. Njegova priča, kao i uloga IT-ja u svakodnevnom funkcionisanju kompanije koja oblači ceo region, osvetljava „digitalnu postavu“ modne industrije, onu koju retko vidimo, ali bez koje bi poslovanje jednostavno stalo. U nastavku razgovaramo sa Dušanom o tome kako IT odgovara na sezone promene, na koji način veštačka inteligencija preporučuje odeću, kako izgleda digitalna transformacija u maloprodaji, i da li bi radije izabrao savršeno funkcionalan ERP ili udobne cipele.

Svaka kompanija je tehnološka kompanija
Kako je Microsoft Certified Business Management Specialist „zalutao“ u kompaniju koja se bavi modom i dizajnom?

Fashion Company jeste u modi i dizajnu kako Vi kažete, no danas je svaka kompanija i tehnološka kompanija.

Nas uglavnom oblikuju naša interesovanja i naša okolina. Još kao dete



Dušan Brdar,
direktor IT sektora
Fashion Company

Više od 80 modnih brendova, preko 2 miliona opcija ide kroz naše sisteme implementirane kroz 18 kompanija i 7 zemalja u ovom trenutku

sam bio očaran novim tehnologijama, a usput sam se negde u hodu susreo sa sjajnim ljudima u *retail* industriji sporta i mode. Imao sam i još uvek imam priliku da sarađujem i učim od najboljih svetskih kompanija poput *Nike*, *Zara*, *PVH*, *Kiko Milano*, *BOSS*, *Replay*, *Mango*. Radim u timu sa izuzetnim kolegama gde stvaramo zajedno novi i bolji *Fashion Company*. Kroz svaki projekat sve više, tehnologija osvaja jednu ovako veliku kompaniju. Mene lično svaka primena naših alata, i direktno ili indirektno bolji rezultat kompanije čine srećnim i motivisanim. Rekao bih da sam „zalutao“ na pravo mesto.

IT u svetu mode često ostaje nevidljiv – kao dobra postava u sakoima. Možete li nam otkriti šta sve čini „digitalnu postavu“ Fashion Company-ja?

Dobra digitalna postava čini firmu da se oseća komforno i sigurno u „našim odelima“, a sve zasluge idu mojim kolegama iz IT sektora. Dva-deset zaposlenih u domenu podrške poslovanju, *competence* centra, infrastrukture, razvojnog i data tima čine neustrašiv tim. Deo naše porodice čini i nekoliko važnih strateških partnera u području razvoja *eCommerce* i *CRM* platforme, *hostinga* i *ERP* konsaltinga. Kako smo regionalna kompanija tako su nam i partneri kompanije koje mogu da nas prate u dinamičnom širenju. IT je, barem u *Fashion Company* veoma bitan i vidljiv faktor koji učestvuje u definisanju razvoja kompanije kroz svoju zastupljenost u bordu kompanije, što se odražava i na veoma visoki plasman

u svetu regionalnih retail kompanija. Mi se tu ne zaustavljamo.

Koji su najveći IT izazovi kada se tehnologija kombinuje sa modnim trendovima koji se menjaju iz sezone u sezonu?

Brzina kretanja kompanije je brža od kretanja modnih trendova te nam ona u većoj meri i diktira neophodni ritam tehnološkog razvoja. Sistemi su nam prilagođeni i skalabilni za prihvatanje skoro neograničenog broja brendova, pa sa te strane smatram da smo u dobroj poziciji. Više od 80 modnih brendova, preko 2 miliona opcija ide kroz naše sisteme implementirane kroz 18 kompanija i 7 zemalja u ovom trenutku. Najveći izazov jeste upravo odgovoriti na brzinu razvoja kompanije koji rešavamo dugoročnim planiranjem, razvojem veština ljudi i strateškim partnerstvima.

Aplikacija koja sve promeni

Da li postoji neka specifična tehnologija – softver, platforma ili sistem – koja vam je promenila način rada u poslednjih nekoliko godina?

Izdvojio bih našu *loyalty* aplikaciju koja se veoma brzo proširila širom regiona i osvojila srca mnogobrojnih članova. Potrudili smo se da korisnicima bude više od klasične aplikacije za kupovinu, te implementirali direktan kontakt sa *customer* servisom na tri načina, naprednu pretragu i pretragu putem AI asistenta tekstom, glasom, fotografijom, kao i razne uvide i editorijale. Razvoj je trajao intenzivno godinu dana i nakon puštanja u rad, aplikacija se konstanto unapređuje i širi kroz nova tržišta. Oslušujemo naše verne kupce i konstantno se trudimo da unapredimo aplikaciju da bude bolja. Saradnja *Fashion Company* i strateškog partnera SyncIT-a je donela sjajne rezultate. Do sada



širom regiona imamo registrovanih preko 500,000 korisnika.

Uz ovu aplikaciju bih dodao da smo implementirali i prve SaaS kase koje smo adaptirali za naše poslovanje uz punu integraciju sa ostalim ekosistemom, a pojedine procese preneli na RPA, razvili svoju aplikaciju koja uspešno kombinuje barkod oznake i RFID tehnologiju, uveli već neizbežne AI alate kojih su pojedine procese u potpunosti preuzeli. Okruženje je veoma dinamično i inovativno i mogao bih još dosta na ovu temu, ipak je red da se završi sa najsajnijim zvezdama, našim *online shopping* destinacijama www.fashionandfriends.com i www.xyzfashionstore.com.

Kanali prodaje

Kako izgleda vaša IT strategija kada su u pitanju omnichannel pristupi – online prodaja, fizičke prodavnice, logistika? Koliko je teško sve to sinhronizovati?

Omnichannel platforma nam je u zadnjih par godina donela značajnu promenu u razmišljanju i procesima. Sada sagledavamo drugačije naše poslovanje. Potrebe naših kupaca nas pokreću, a upravo iz tih razloga vođeni savetima i željama, smo transformisali poslovanje iz klasičnog *retailera* i nezavisnog *eCommerce* kanala u „jedan svet“ – *omnichannel*. On nam je doneo mnoštvo izazova,

Naša *loyalty* aplikacija se veoma brzo proširila širom regiona i osvojila srca mnogobrojnih članova. Potrudili smo se da to bude više od klasične aplikacije za kupovinu, te implementirali direktan kontakt sa *customer* servisom na tri načina, naprednu pretragu i pretragu putem AI asistenta tekstom, glasom, fotografijom, kao i razne uvide i editorijale

novih procesa i drugačiji pristup razvoju. Te promene još uvek traju i čine nas potpuno drugačijom kompanijom.

Veza između svih segmenata poslovanja jeste postojala i ranije, no sa novom dinamikom i potrebama da se našim kupcima pruži najbolje iz oba sveta dovela je do daleko bolje povezanosti i češće interakcije. Interno razvijeni OMS, pružanje uvida u jedinstvene zalihe po svakom objektu, alata kako za malo-prodaju tako i za timove u direkciji, dodatna povezanost sa mnogobrojnim partnerima za 3pl i kurirske usluge, marketing i AI alati, napredni CRM, izmene na BI analitici i mnogo toga još je kreirano kao temelj za bolje iskustvo naših kupaca. *Omnichannel* komponenta je obuhvaćena kroz strategiju rasta i daljeg razvoja našeg tehnološkog steka, te se svi alati sa tim na umu planiraju i razvijaju.

Rezultati u maloprodaji trenutno imaju trend stagnacije, što nije pravilo već posledica trenutnog ekonomskog stanja. U *eCommerce* kanalu je vidljiv trend rasta od 4% do 22% u zavisnosti od tržišta. Klasičan *brick and mortar* kanal je ostao destinacija gde ljudi i dalje vole da kupuju, a uprkos očekivanjima da će mlađe generacije prebaciti sve na *online*, ovo

pretskazanje se nije ostvarilo. U *fashion retail*-u još uvek ne postoji digitalno rešeno čulo dodira, dok sama virtualna proba artikala za mnogobrojne alate i dalje ne daje verodostojnu sliku. Uzimajući u obzir i navike generacije Z gde se često druže i organizuju posete tržnim centrima, smatram da je klasičan *retail* tu da ostane. Ponovimo intervju za 5 godina kako bi sagledali šta se desilo.

Snaga veštačke inteligencije

AI je sve prisutniji u analizi podataka, pa i u preporukama proizvoda. Da li koristite veštačku inteligenciju da predložite kupcima savršeni outfit? Hoće li se AI koristiti sve više?

AI je sada prisutan svuda i upitna je samo naša percepcija da se negde ne može upotrebiti. Naravno pričam o našem poslovanju. Preporuke i pretrage proizvoda kroz kontekst, video i audio opcije su odavno prisutne na našem AI *Athena search engine*-u u okviru eCommerce platforme. Pored toga radimo upravo i na uvođenju takvih opcija i u fizičkim radnjama za koje se nadam da će dodatno pojačati korisničko iskustvo. Čitav segment AI generisanja sadržaja nam je veoma interesantan i ulažemo dosta u razvoj i poboljšanje alata u ovom segmentu. Što se tiče samih predikcija i pomoći AI-ja za dobijanje boljih uvida, nadam se da ćemo uskoro imati da se pohvalimo dobrim rezultatima. Ovo polje jeste jedno od najinteresantnijih i nosi mnogobrojne ideje. Ipak brzina i nepromišljene odluke mogu doneti i izazove. Zato ovoj temi pridajemo posebno mesto u strategiji.

U modnom svetu se stalno govori o stilskim ikonama. Da li i u IT svetu imate svoje uzore – stilove kodiranja, omiljene framework-e, klasične tehnologije koje su uvek u modi...

Agile metodologija upravljanja i razvoja je naš *framework*. Ova metodologija je pokazala najbolje rezultate i van okvira IT-ja. S obzirom na to da imamo više timova, metodologija je adaptirana prema potrebama kompanije. Alati koji u najvišoj meri koristimo jesu C#, Kotlin, C/AL i T-SQL. Kako je kod nas u regionu sve



Klasičan „brick and mortar“ kanal je ostao destinacija gde ljudi i dalje vole da kupuju, a uprkos očekivanjima da će mlađe generacije prebaciti sve na online, ovo pretskazanje se nije ostvarilo

Mi jesmo tehnološki sektor, ali u okviru *retail* kompanije, gde živimo sa, i u industriji. Često upotrebim izraz da smo mi „primenjeni IT“

veći broj *Python* stručnjaka, mislim da ćemo mu i mi pružiti šansu.

Ako biste morali da napravite analogiju između modnog brenda i IT tehnologije, da li bi SAP bio Armani, a Shopify neka brža Zara?

Sjajno pitanje, na koje nisam siguran šta bih odgovorio no pokušaću. Mi koristimo za poslovanje *Business Central* (nekadašnji *Navision*) koji je veoma lagan, brz za razvoj i priliči agilnoj firmi. Podseća me na mladalački brend pa bih ga uporedio recimo sa brendom *Replay*. SAP je ipak sličniji nekom velikom sistemu koji se dokazivao i pokazivao godinama te bih ga uporedio sa brendovima kao što su BOSS ili *Tommy Hilfiger*. *Magento* koji koristimo za eCommerce me najviše podseća na *Scotch&Soda*, dok me *Shopify* podseća na *Kiko Milano*, naš *make-up* i *skin care* brend.

Spremni za sezone udare

Moda je brza, ali IT mora biti brži. Kako održavate infrastrukturu da bude spremna za sezone udare – popuste, nove kolekcije, praznične kupovine...

Pre dve godine smo kompletnu infrastrukturu *outsource*-ovali kod private cloud provajdera. U okviru projekta smo celokupnu infrastrukturu ponovo podigli i kreirali je skalabilnom. Ipak sem same skalabilnosti infrastrukture, u okviru tekućeg poslova radimo na konstantnom unapređenju postojećih procesa, na usvajanju novih tehnologija, novih pristupa, radimo na *refactoring*-u koda i na taj način doprinosimo bržem i stabilnijem poslovanju.

Da li postoji neka IT funkcionalnost ili rešenje koje ste vi „progrurali“ u firmi, a sad ne možete da zamislite poslovanje bez toga?

IT u našoj kompaniji je sektor koji učestvuje u kreiranju velikog broja procesa, kako kroz ERP, maloprodajni softver, tako i kroz ostale aplikacije. Mnogo ideja je došlo iz razgovora i interakcije sa našim kolegama i partnerima širom regiona. Tajni začim jeste zajednički prostor i svakodnevna interakcija u kancelarijama i hodnicima, na pauzama i sastancima, na „afteru“ u pivnici ili kafiću, brainstormingu gde god se skupimo. Moja uloga, među ostalim, i jeste da prepoznajem i „guram“ dobre ideje zarad dobrih kompanije. Od dobrih ideja, hajde da izdvojimo da jedna na izgled malena aplikacija *RunnerApp* koja pomaže bržoj usluzi kupaca jeste sada neizostavni deo našeg u poslovanja. AI *content* aplikacija je inovirala u potpunosti procese izrade contenta. OMS (*Order management System*) je interno razvijen i postao je um, kontrola i realizacija milijardi transakcija.

Veoma je važan taj faktor da mi jesmo tehnološki sektor ali u okviru *retail* kompanije, gde živimo sa, i u industriji. Često upotrebim izraz da smo mi „primenjeni IT“.

Za kraj – šta biste radije imali: savršeno funkcionalan ERP ili par savršeno udobnih cipela?

Ispred svega bih uvek izabrao savršeno funkcionalan tim, a zatim bih kupio te cipele... Za kraj bih citirao vlasnika kompanije: „Sa ljudima se možeš popeti i na Mesec.“

Sve što ti treba za tvoj podcast

Snimi svoj podcast koji
zvuči i izgleda profesionalno



3 kamere za
dinamičan video



3 mikrofona i
2 miksete za
besprekoran zvuk



**Profesionalna
rasveta**



Operateri koji vode
snimanje i tehniku

Bez skrivenih troškova. **Bez glavobolje.** Samo vi i vaša ideja.

Samo 8.990 po satu

+ Montaža dostupna po dogovoru – niste prepušteni sami sebi

PC Press studio u centru Beograda.
Rezervišite termin: **011/20-80-220** ili marketing@pcpress.rs

Vi donesite priču. Mi ćemo je snimiti.

Beauty Tech u centru industrije lepote

Veštačka inteligencija, proširena stvarnost i održive inovacije menjaju lice industrije lepote. Personalizovana rešenja, pametni uređaji i digitalni asistenti postaju deo svakodnevice, dok brendovi poput L'Oréal-a predvode revoluciju u kojoj se tehnologija, nauka i kreativnost spajaju da bi oblikovali budućnost lepote

✉ Marijana Pečić

Industrija lepote nalazi se usred najveće digitalne transformacije do sada. Tehnologija, nauka i kreativnost više nisu pomoćna sredstva - danas su glavni pokretači promena koje redefinišu proizvode, usluge i korisnička iskustva. Trendovi pokazuju da se budućnost lepote gradi na personalizaciji, inkluzivnosti i održivosti, a sve to uz snažan oslonac na napredna digitalna rešenja.

Nove generacije potrošača, nove potrebe

Savremeni potrošači očekuju mnogo više od estetskog efekta. Traže proizvode i usluge koji odgovaraju njihovim individualnim karakteristikama - od tipa kože i kose, preko životnih navika, do ličnih stilskih afiniteta. Istovremeno, raste svest o održivosti, ekološkom otisku i društvenoj odgovornosti brendova.

Do 2030. godine čak 40 odsto svetske populacije imaće talasastu, kovrdžavu ili loknastu kosu, dok će dve trećine imati melaninom bogatu kožu sa specifičnim potrebama nege. Uz to, urbanizacija i klimatske promene uvode nove izazove, poput zagađenja i povećane UV izloženosti, pa potrošači traže rešenja koja ne samo da ulepšavaju već i štite zdravlje kože i kose.

La Roche Posay
Spotscan coach



Tehnologija u službi personalizacije

Digitalna revolucija otvorila je vrata ekstremnoj personalizaciji. Uređaji kao što je *Lancôme Cell BioPrint* analiziraju biološku starost kože za svega pet minuta, koristeći naprednu proteomiku i AI algoritme, i daju individualne preporuke proizvoda i tretmana.

Virtuelni *try-on* sistemi, bazirani na tehnologijama proširene stvarnosti (AR), omogućavaju korisnicima da isprobaju različite *make-up* i *hair* varijante bez fizičkog testiranja proizvoda. *Modiface*,

L'Oréal-ova AR platforma, koristi više od 65 preciznih tačaka lica i trenirana je na hiljadama fotografija različitih tipova kože, starosnih dobi i polova, kako bi virtuelno isprobavanje bilo maksimalno realistično.

Ovakva rešenja ne samo da unapređuju korisničko iskustvo već i znatno smanjuju potrebu za testnim uzorcima, doprinoseći održivosti.

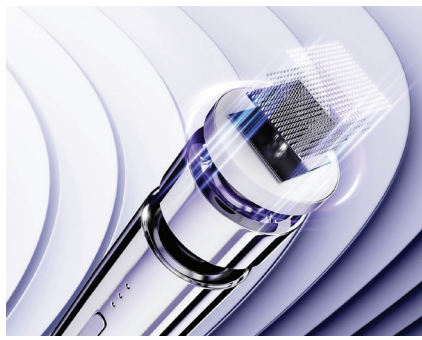
L'Oréal-ove AI dijagnostike idu korak dalje - u saradnji s *Google Maps* platformom analiziraju podatke o kvalitetu vazduha, UV indeksu i vremenskim uslovima kako bi personalizovali preporuke, dok partnerstvo sa aplikacijom *Clue* pruža uvid u uticaj menstrualnog ciklusa na kožu. Rezultat su ultrapersonalizovana rešenja koja na prodajnim mestima dovode do konverzije od čak 70 odsto.

AI kao novi kreativni partner

Veštačka inteligencija više nije samo alat za obradu podataka - ona postaje kreativni partner istraživačima i brendovima. *L'Oréal* i IBM razvijaju prvi AI *foundation* model u kozmetičkoj industriji, koji omogućava identifikovanje novih formulacija sa održivim sirovinama, skraćuje razvojni ciklus i smanjuje potrošnju energije i otpada. U oblasti boja za kosu, AI ubrzava razvoj novih nijansi i do 50 odsto, kombinovanjem prediktivnih modela i mašinskog učenja.



Uređaj Lancôme Cell Bioprint analizira biološku starost kože za svega pet minuta



Lancôme Renergie Nano - Resurfacer 400 booster omogućava dublju aplikaciju seruma



Water saver tuš razvijen sa startapom Gjosa omogućava salonima da uštede do 69% vode po pranju kose

Generativni AI koristi se i u *CreAI-tech* laboratoriji za kreiranje vizuala i kampanja u skladu s principima odgovornog oglašavanja, bez korišćenja AI generisanih „lica“ i „tela“ za prikaz svih prednosti proizvoda. Alat BETiq optimizuje raspodelu marketinških budžeta, povećavajući ROI.

Održivost kao strateški prioritet

Održiva inovacija postaje centralni deo *beauty tech* agende. Rešenja poput *Water Saver* tuša, razvijenog sa startapom *Gjosa*, omogućavaju frizerskim salonima da uštede do 69 odsto vode po pranju kose, a već su sačuvali više od 530 miliona litara vode širom sveta.

AirLight Pro fen kombinuje infracrveno svetlo i optimizovan protok vazduha, suši kosu 21 odsto brže, uz 55 odsto veću hidrataciju i 19 odsto manju potrošnju energije.

Vertikalne farme *BioPods*, vođene AI sistemima, omogućavaju kontrolisani uzgoj biljnih sastojaka s minimalnom potrošnjom resursa, a inovacija *Osmobloom™* uvodi novu eru u kreiranju parfema hvatanjem mirisa iz prirode bez oštećenja biljaka.

Pametne usluge i digitalni asistenti

Beauty tech donosi i novu generaciju usluga. *L'Oréal Paris Beauty Genius*, razvijen u partnerstvu s *Metom*, funkcioniše kao 24/7 personalni asistent dostupan na *WhatsApp*-u, nudeći personalizovane preporuke i odgovore na pitanja korisnika. *La Roche-Posay Spotskan+ Coach* povezuje dermatološku analizu s

programima za mentalno zdravlje, nudeći i meditacije kroz saradnju sa aplikacijom *Calm*. *Noli* koristi bazu s više od milion skeniranih lica i analizu hiljada preporuka proizvoda kako bi potrošačima pomogao da donesu najbolje odluke. *HAPTA*, prvi AI aplikator šminke za osobe sa ograničenom pokretljivošću, vraća samostalnost u svakodnevnoj nezi i dobio je priznanja kao jedan od najznačajnijih izuma godine.

U domenu kućne nege, uređaji kao što je *Colorsonic* nude precizno farbanje kose kod kuće bez nereda, dok *Lancôme Rénergie Nano-Resurfacer 400 Booster* omogućava dublju apsorpciju seruma korišćenjem nanočip tehnologije s mikroiglicama.

Loreal Groupe
Vertical farming
BioPods vođene AI sistemima



L'Oréal - od pionira do lidera u beauty tech-u

Od prve sigurne boje za kosu koju je 1907. godine stvorio osnivač *Eugene Schueller*, do današnjeg liderstva u AI i AR rešenjima, *L'Oréal* kontinuirano pomera granice inovacija. Nedavno proglašena za najinovativniju kompaniju u Evropi prema listi magazina *Fortune*, kompanija gradi strategiju na tri stuba: nauci, tehnologiji i kreativnosti. Takođe, kompanija danas ima više od 90.000 zaposlenih, prisutna je u 150+ zemalja i okuplja 37 brendova. U 2024. godini prijavila je 694 patenta, zabeležila 110+ miliona korišćenja svojih *beauty tech* servisa, angažovala 8.000 digitalnih, tehnoloških i *data* stručnjaka i izgradila najveću svetsku bazu *beauty* podataka - 14.500 terabajta, uz 60 odsto žena u novim *tech/data* timovima.

Učešće na sajmovima kao što su CES i *Viva Technology* pozicionira je ne samo kao *beauty* brend već i kao tehnološkog lidera čije inovacije imaju primenu i van kozmetičkog sektora. *L'Oréal x Meta* program doneo je više od 50 kampanja kreiranih s digitalnim umetnicima, koje su ostvarile preko 100 miliona pregleda na mrežama. *Beauty Tech* više nije u zapećku industrije, već u njenom centru. Tehnologija ne menja samo proizvođače već i način na koji doživljavamo lepotu, kupujemo i brinemo o sebi. Personalizovana rešenja, održivi procesi i digitalni asistenti postaju standardi koje potrošači očekuju. A kompanije koje uspeju da spoje nauku, tehnologiju i kreativnost, kao što to radi *L'Oréal*, oblikovaće lice lepote - i biznisa - u decenijama koje dolaze.

 www.loreal-paris.rs