Specijalni dodatak časopisa PC Press

PC PRESS

www.pcpress.rs

Izazovi savremenih data centara

NAS na AI steroidima

Data centri i veštačka inteligencija

Data centri 2024

Data centar gradivni element poslovanja

Modernizacija **i pouzdanost data centara**

Zaštita tajnih i poverljivih informacija nikada nije bila važnija za organizacije

Možete li zamenom **starog UPS uređaja za novi da uštedite novac?**

Prednosti mikro data centara u teškim industrijskim i komercijalnim okruženjima

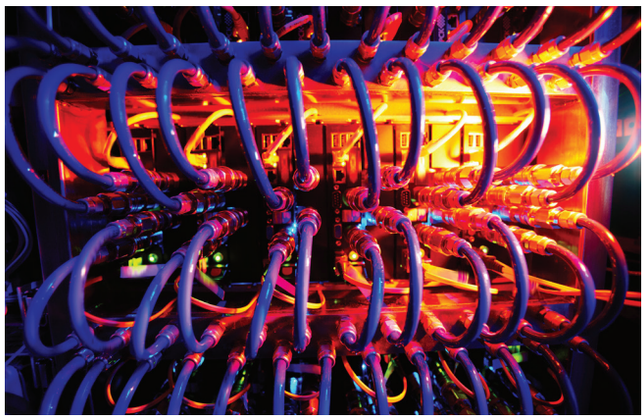
Upravljanje sajberbezbednošću

Data centar – gradivni element poslovanja

Koji je zajednički imenitelj kupovine preko Amazon-a, Ali-ja ili eBay-a, čuvanja podataka u cloud-u, pretraživanja Google-a, zadavanja pitanja AI ChatBot-ovima i gledanja filmova na streaming platformama? Praktično sve što danas radimo, kao pojedinci ili kompanije, zasnovano je na data centrima ili, kako ih još zovu, centrima podataka

Branislav Bubanja

Data centar je objekat, zgrada ili zakupljen prostor, sastavljen od umreženih računara, sistema za smeštanje podataka sistema i računarske infrastrukture koje kompanije upotrebljavaju za čuvanje, obradu i deljenje velike količine podataka. Kompanije se danas uglavnom oslanjaju na aplikacije, usluge i podatke koji se čuvaju u *data* centrima i zato možemo da kažemo da su oni neophodan sastojak svakog IT poslovnog okruženja.



Ekosistem podataka

Data centar ne podrazumeva samo gomilu servera koji čuvaju i obrađuju podatke. To je čitav ekosistem koji, pored računara, obuhvata i fizičku infrastrukturu koja ih povezuje, ali i pomoćne sisteme sačinjene od električnih instalacija, infrastrukturu za održavanje konstantne temperature i vlažnosti vazduha, te infrastrukturu za fizičko obezbeđivanje podataka.

Pošto se u *data* centrima obavljaju gotovo sve operacije i u njima se čuvaju svi poslovni podaci i pokreću aplikacije neophodne za obavljanje poslovnih procesa, jasno je da oni danas predstavljaju jedan od najbitnijih elemenata koji obezbeđuje uspešnost poslovanja. „Pad“ *data* centra prouzrokovao bi potpuni zastoj poslovanja kompanije. Zato u njima važe posebni bezbednosni protokoli koji obuhvataju sve segmente, od fizičkog obezbeđenja prostora u kome se *data* centar nalazi, do obezbeđenja podataka koji se čuvaju u njemu.

AI tehnologije zahtevaju ogromnu računarsku snagu, prostor za skladištenje i umrežavanje s malim kašnjenjem za obuku i pokretanje modela. Obično se AI aplikacije hostuju u samim data centrima

Bezbednost u *data* centrima možemo da podelimo u četiri segmenta koji zajedno čine neraskidivu celinu. Obezbeđenje prostora odnosi se na zaštitu pristupa lokaciji u kojoj se nalazi infrastruktura i oprema *data* centra. Sistemi za skladištenje i obradu podataka su obavezno redundantni, a *backup* sistemi se nalaze na udaljenim lokacijama – u drugim gradovima, državama, pa čak i na drugim kontinentima. Na taj način se osigurava funkcionisanje *data* centra i u slučaju prirodne ili neke druge nepogode na jednoj od lokacija.

Još jedan od bezbednosnih parametara *data* centra jeste instalirana prateća infrastruktura koja treba da obezbedi maksimalnu održivost i postojanost *data* centra. Pod pratećom infrastrukturom podrazumevaju se sistemi za distribuciju električne energije, rezervni generatori, UPS-evi, sistemi za hlađenje, ventilaciju, opremu za povezivanje na Internet... I konačno, neizostavni deo svakog *data* centra čine zaposleni koji su zaduženi za održavanje i nadgledanje svih prethodno pomenutih komponenti.

Vrste data centara

Postoji nekoliko vrsta *data* centara, koji se razlikuju u zavisnosti od veličine, lokacije, kapaciteta, zahteva poslovanja, vlasništva, kao i nekih drugih parametara.

Lokalne *data* centre kompanije grade za sopstvene potrebe ili za potrebe njihovih korisnika. Sve aplikacije, kao i podaci koji se obrađuju, nalaze se unutar tog *data* centra, koji je najčešće fizički lociran u okviru same kompanije. Iznajmljeni *data* centri su specijalizovani za iznajmljivanje resursa. Za njihovo održavanje odgovorni su vlasnici *data* centra, a ne kompanije koje ih iznajmljuju. Ovo rešenje je posebno pogodno za manje kompanije koje nemaju dovoljno resursa da vode sopstvene *data* centre, ili koje žele da smanje inicijalne troškove uspostavljanja *data* centra.

Cloud data centri su distribuirani *data* centri smešteni van kompanije. Njima upravljaju nezavisni *cloud* provajderi, a najpoznatiji su *Amazon Web Services*, *Microsoft Azure* i *Google Cloud*. Ove *data* centre treba

razlikovati u odnosu na iznajmljene *data* centre, jer su zasnovani na *Infrastructure-as-a-Service* modelu. Zahvaljujući tome, kompanije mogu da veoma brzo i jednostavno kreiraju sopstvene virtuelne *data* centre.

U praksi je čest primer kombinovanja iznajmljenih i lokalnih *data* centara. Ova vrsta *data* centra naziva se kolokacijski *data* centar. Njegova specifičnost je što se lokacija *data* centa nalazi u vlasništvu neke druge kompanije, dok su oprema, hardver i kompletna infrastruktura u vlasništvu kompanije koja je iznajmila prostor na toj lokaciji. Ovakav *setup* je zgodan za kompanije koje žele da imaju sopstvene *data* centre, ali i da smanje troškove vezane za izgradnju i održavanje lokacije u kojima bi se oni nalazili.

Edge data centri su najčešće manji objekti lokacijski postavljeni kod korisnika *data* centara. Time se rešava problem kašnjenja, jer se takvi *data* centri nalaze praktično na izvoru podataka i ne zavise od veze sa Internetom.

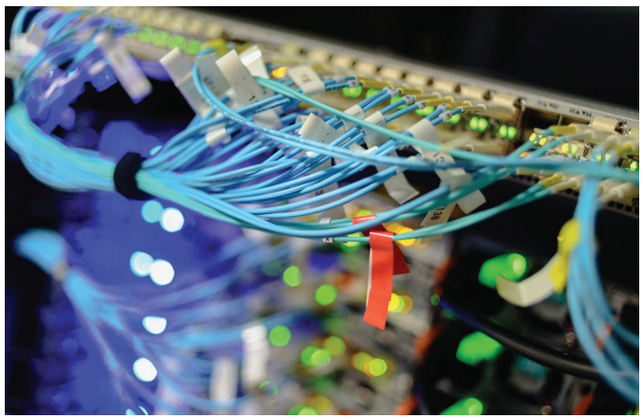
I konačno, postoje *hiperscale data* centri. To su ogromni *data* centri koje poseduju globalne IT kompanije, napravljeni za masivne obrade podataka. Infrastruktura ovih *data* centara je napravljena da maksimizuje gustinu hardvera, uz minimizovanje administrativnih troškova i troškova funkcionisanja (hlađenja, električne energije). Da bi to postigli, ovakvi *data* centri koriste inovativne tehnike i „zelene“ tehnologije. Na primer, energiju dobijaju solarnim putem, nalaze se ispod površine vode kako bi obezbedili efikasnije hlađenje. Takve *data* centre poseduju globalne kompanije kao što su *Google*, *Meta*, *Amazon*, *Microsoft*, *Apple*...

Podela prema nivoima

Osim po veličini i načinu upotrebe, jedna od najčešćih podela *data* centara je po nivoima (TIER-ima). Pre 19 godina *American National Standard Institute* (ANSI) je, u saradnji s *Telecommunications Industry Association* (TIA), objavio ANSI/TIA-943 standard koji definiše četiri nivoa dizajna i implementacije *data* centara. Ti nivoi su zasnovani na dostupnim resursima, kapacitetima i garantovanom vremenu rada. *Uptime Institute* je na osnovu tog standarda definisao četiri tipa *data* centara.

TIER I *data* centri su osnovni tip. Oni moraju da poseduju UPS, ali ne i redundantne sisteme. Garantovano vreme rada je 99,671%. TIER II *data* centri moraju da imaju redundantne servere, kao i sisteme napajanja i hlađenja. Garantovano *up-time* vreme kod ovog nivoa mora da bude 99,741 procenata. TIER III *data* centri moraju da obezbede energetsku samostalnost od 72 sata, uz potpunu redundantnost svih sistema i delimičnu toleranciju na greške. Minimalno vreme rada kod ovog nivoa je deklarisano na 99,982 procenta.

Najviši nivo, TIER IV *data* centri, obezbeđuju potpunu redundantnost i energetsku samostalnost od 96 časova, uz minimalno vreme aktivnosti od 99,995 procenta. To znači da vreme ukupne neaktivnosti na godišnjem nivou kod TIER IV *data* centra ne sme da bude duže od 26,3 minuta!



Infrastruktura data centara

Infrastrukturu *data* centra čine fizički elementi od kojih je on sastavljen. Serveri su svakako njen najvažniji deo, ali su serveri beskorisni bez ostalih infrastrukturnih elemenata. Fizička infrastruktura, u najgrubljem smislu, podeljena je na IT hardver i hardver za podršku. IT hardver čine pomenuti serveri, ruteri, svičevi, sistemi za smeštaj i čuvanje podataka, *failover* sistemi, redundantna napajanja, mrežni i strujni kablovi koji sve to povezuju... Hardver za podršku čine svi oni sistemi koji su sastavni deo *data* centra, ali ne potpadaju pod IT opremu. To su sistemi za ventilaciju i hlađenje, protivpožarni sistemi, bezbednosni sistemi (kamere, senzori)...

IT hardver čine serveri, ruteri, svičevi, sistemi za smeštaj i čuvanje podataka, failover sistemi, redundantna napajanja, mrežni i strujni kablovi koji sve to povezuju

Data centar je veoma širok pojam i može da podrazumevaju nekoliko malih umreženih servera smeštenih u nekoj kancelariji kompanije, ili čak i u kontejneru (za njih se koristi izraz „*data center in a box*“). Takvi *data* centri su u neku ruku mobilni, jer lako mogu da se premeste na drugu lokaciju gde će veoma brzo ponovo biti aktivni.

Na drugom kraju liste nalaze se veliki *data* centri, koji mogu da zauzimaju ogromna skladišta sa specijalizovanom opremom i infrastrukturom. Primer imamo i kod nas – Državni data centar u Kragujevcu. Otvoren je u decembru 2020. godine i predstavlja najsavremeniji objekat tog tipa u regionu. Prostire se na površini od četiri hektara, a čine ga dva objekta ukupne površine 14.000 kvadratnih metara. Projektovan je i izgrađen po najvišim tehničkim i bezbednosnim standardima i potpada u TIER IV kategoriju, a kapacitet mu je 1080 *rack* ormara.

Vreme ukupne neaktivnosti TIER IV data centra na godišnjem nivou ne sme da bude duže od 26 minuta!

Veštačka inteligencija i data centri

Sveopšti hajp oko AI tehnologija ima ogroman uticaj i na *data* centre. AI tehnologije zahtevaju ogromnu računarsku snagu, prostor za skladištenje i umrežavanje s malim kašnjenjem za obuku i pokretanje modela. Obično se AI aplikacije hostuju u samim *data* centrima, zbog dostupnosti resursa i optimizovanih uslova rada. Kako veštačka inteligencija nastavlja da dobija sve širu primenu, tako će se proširivati i zahtevi u *data* centrima za tu namenu.

AI može da utiče na *data* centre na još nekoliko načina. On omogućava stvaranje inteligentnih *data* centara koji su optimizovani i automatizovani upotrebom veštačke inteligencije, mašinskog učenja i IoT uređaja. Zahvaljujući ovim tehnologijama, mogu da se poboljšaju ključni aspekti rada *data* centara – upravljanje resursima, bezbednost i efikasnost, uz poboljšanje ukupnih performansi *data* centra i optimizaciju troškova.

Modernizacija i pouzdanost data centara

U današnjem digitalnom dobu, gde brz razvoj tehnologije i novih IT trendova dovodi do višestruko multiplikovanih količina podataka i informacija, uloga data centara postaje sve značajnija za funkcionisanje savremenog načina života

Nebojša Ćosović, direktor sektora usluga, kompanija ENEL PS

Veštačka inteligencija (AI), virtuelna realnost (VR), IoT (*Internet of Things*), *cloud*, *edge*, 5G, *Blockchain*, Industrija 4.0 i mnoge druge nove industrije kreiraju dodatne zahteve za energijom, a zahtevi za energetskom efikasnošću i održivošću takođe postaju sve važniji faktori, dok starost postojećih *data* centara može biti izazov zbog smanjene efikasnosti i pouzdanosti starije opreme.

Naravno, dostupnost i besprekidan rad *data* centra se podrazumevaju.

Modernizacija sistema za preciznu klimatizaciju

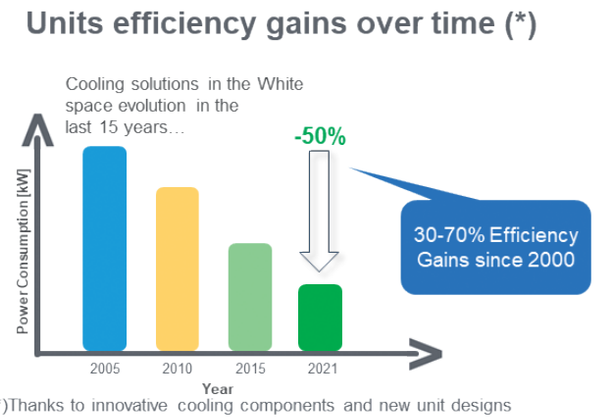
U *data* centru najveću potrošnju električne energije, ne računajući IT opremu, ima klimatizacija. Procene se kreću od 30-40 odsto od ukupne potrošnje.

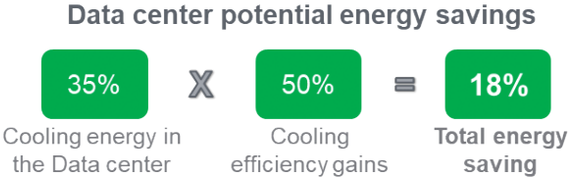
Treba imati na umu da je u prethodnih 15 godina došlo do evolucije u dizajnu i komponentama sistema za klimatizaciju, kao što su:

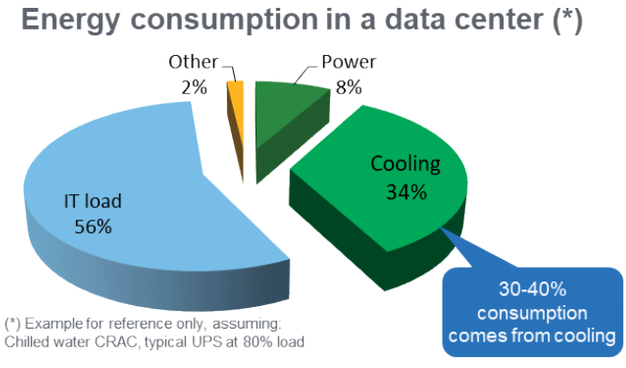
- ventilatori sa EC motorima i prilagođenim elisama koje smanjuju buku i gubitke,
- ventilatori i pumpe s varijabilnim brzinama rada,
- *brushless* kompresori s varijabilnim brzinama rada,
- elektronski ekspanzioni ventili za upravljanje freonom,
- upotreba freona s najmanjim GWP indeksom i najmanjim uticajem na životnu sredinu,
- inovativni sistemi *free cooling*-a,
- strategije distribucije vazduha uz zatvaranje tople ili hladne zone.

Procenjuje se da su savremeni sistemi za klimatizaciju od 30 do 70 odsto energetski efikasniji od sistema starije generacije.

Ukoliko to preračunamo na prosečnu tipičnu potrošnju sistema za klimatizaciju u okviru *data* centra, dolazimo do procenjene moguće uštede od 18 odsto modernizacijom sistema za klimatizaciju.







Inteligentni sistem za adijabatsko hlađenje čilera

Dodatni način za unapređenje efikasnosti sistema za hlađenje je upotreba Inteligentnog sistema za adijabatsko hlađenje čilera.

Sistem adijabatskog hlađenja na čilerima je tehnologija koja funkcioniše tako što koristi adijabatski proces, što znači da se vazduh hladi putem isparavanja vode.

U suštini, voda se raspršuje u vazduh koji prolazi kroz čiler, što rezultira smanjenjem temperature vazduha pre nego što uđe u sam čiler. Kada ovako prethlađeni vazduh uđe u čiler, manje je potrebno hladiti ga kako bi se postigla željena temperatura za proces hlađenja. To znači da čiler radi s manje napora, što dovodi do smanjenja potrošnje električne energije i bolje energetske efikasnosti sistema za klimatizaciju, ali i manjeg habanja svih delova sistema.

Reduce chiller electricity consumption **by up to 37%**

Increase cooling capacity **by up to 41%**

Gain **total condenser protection**

Ovaj sistem adijabatskog prethlađenja vazduha može biti koristan posebno u područjima gde je vazduh veoma topao i suv. Takođe, može biti deo održivih pristupa hlađenju, jer smanjenjem potrošnje energije doprinosi smanjenju emisije štetnih gasova i negativnog uticaja na životnu sredinu što nam je jedan od prioriteta u kompaniji ENEL PS.

EcoStruxure IT Cooling Optimize

Još jedan od načina za unapređenje efikasnosti hlađenja u *data* centru je korišćenje *EcoStruxure* IT *Cooling optimize* rešenja.

- *Cooling optimize* modul u okviru *EcoStruxure* IT platforme predstavlja naprednu funkcionalnost koja doprinosi unapređenju efikasnosti hlađenja u *data* centrima na nekoliko načina:
- *Cooling Optimize* AI (*Artificial intelligence*) modul koristi senzore i analizira podatke o temperaturi u *data* centru kako bi prilagodio rad sistema za hlađenje i omogućio tačno dovoljnu količinu hlađenja koja je potrebna na mestima gde je to potrebno. Ovakvim načinom rada, modul može dinamički prilagođavati postavke hlađenja kako bi održao optimalnu temperaturu u prostoriji, minimizirajući prekomerno hlađenje i smanjujući potrošnju energije.

Modul koristi algoritme za optimizaciju rada sistema za hlađenje kako bi maksimizovao efikasnost i minimizirao potrošnju energije. Na osnovu podataka o opterećenju i temperaturi, modul može dinamički prilagođavati brzinu ventilatora, temperaturu rashladnog fluida i druge parametre kako bi obezbedio optimalne uslove hlađenja uz minimalnu potrošnju energije.

EcoStruxure IT platforma predstavlja skup moćnih alata za upravljanje i nadzor IT infrastrukturom, koji omogućava korisnicima da efikasno upravljaju, nadgledaju i analiziraju svoje IT resurse, poboljšavajući pouzdanost, efikasnost i performanse svoje IT infrastrukture.

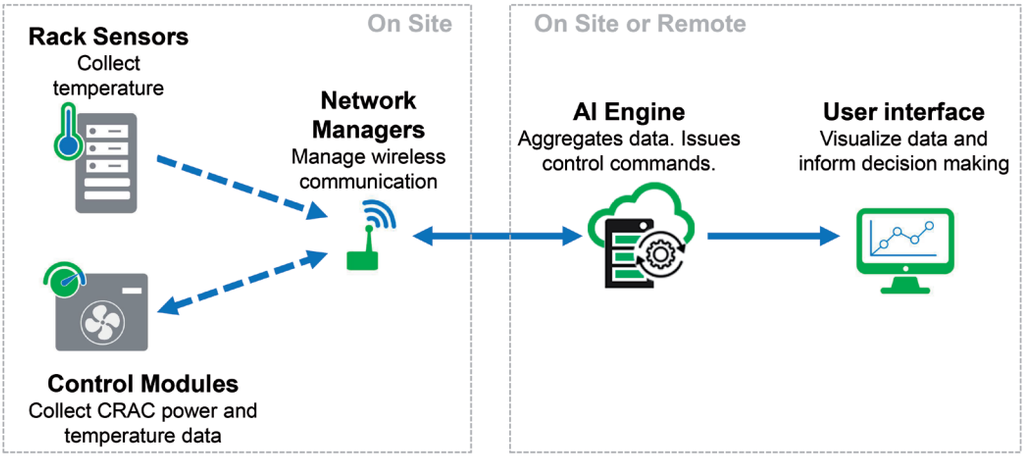
Jedna od ključnih funkcija *EcoStruxure* IT *Expert*-a je kontinuirano praćenje i analiza podataka o performansama IT infrastrukture, uključujući energetske parametre, temperature, opterećenja opreme i druge relevantne metrike. Na osnovu ovih podataka, korisnici mogu dobijati detaljne informacije o stanju svoje IT infrastrukture, identifikovati potencijalne probleme ili rizike i preduzeti odgovarajuće korake kako bi obezbedili neprekidan rad i optimalne performanse.

U data centru najveću potrošnju električne energije, ne računajući IT opremu, ima klimatizacija. Procene se kreću od 30-40 odsto od ukupne potrošnje

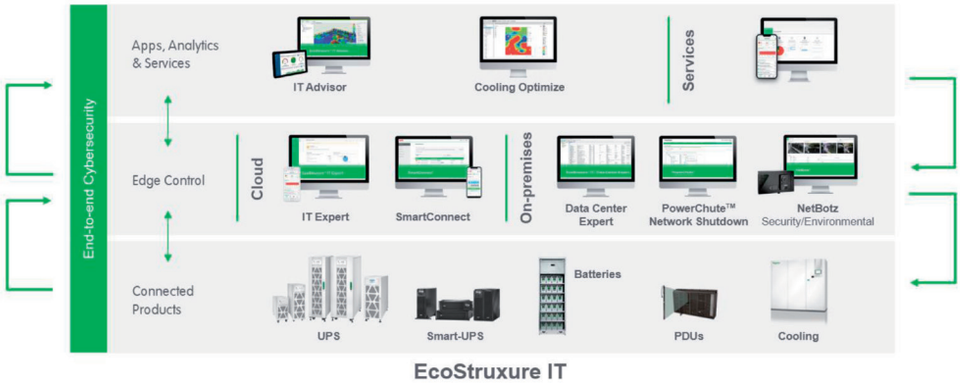
ENEL PS postavlja standarde u industriji servisiranja *data* centara kroz primenu gorenavedenih rešenja, posvećeni smo inovacijama, unapređenju energetske efikasnosti i neprekidno ulažemo u razvoj novih tehnologija i rešenja. Sa 30 godina iskustva i uspeha iza sebe, ENEL PS ostaje pouzdan partner svojim klijentima u njihovoj digitalnoj transformaciji i ostvarivanju poslovnih ciljeva.

enelps.com

What are the components of the system?



The EcoStruxure IT Platform delivers enhanced visibility and management



EcoStruxure IT

Novo rešenje za hlađenje koristi vodu za jednofazno direktno tečno hlađenje

Rittal je razvio megavatno hlađenje za AI

Veštačka inteligencija (AI) obećava revolucionarnu korist. Da li je IT infrastruktura spremna? Operatori data centara probijaju novi tehnološki teren sa svojim tehnološkim partnerima. Predstavljamo vam novo rešenje za hlađenje koje isporučuje više od jednog megavata hlađenja i utire put veštačkoj inteligenciji

Potražnja za računarskom snagom raste toliko brzo da je potreban potpuno novi nivo skalabilnosti, hlađenja, distribucije električne energije i energetske efikasnosti. *Rittal* kao globalni proizvođač IT infrastrukture na taj način ulazi u novo i još šire polje IT hlađenja, u smislu performansi i tehnologije.

Prilike koje nudi veštačka inteligencija deluju gigantski. U junu 2023. godine, *McKinsey* je predvideo da bi povećana produktivnost koju je doneo *GenAI* mogla da doda između 2,6 i 4,4 triliona dolara godišnje globalnoj ekonomiji. Ako bi se i delić toga mogao realizovati, IT infrastruktura bi mogla da raste što je brže moguće i da bude tehnološki imperativ u ključnim oblastima.

U bliskoj saradnji s nekoliko hiperskalera, *Rittal* je razvio modularno rešenje za hlađenje koje isporučuje kapacitet hlađenja od više od 1 MW s direktnim vodenim hlađenjem. Potreban je visok nivo standardizacije i skalabilnosti kroz modularni dizajn i globalnu dostupnost kako bi se omogućila brza ekspanzija infrastrukture tehnički, ekonomski i organizaciono.

Modularna platforma za jednofazno direktno vodeno hlađenje

Rittal koristi rashladne jedinice za jednofazno direktno tečno hlađenje

risnike jer će biti potrebne sve veće performanse i skalabilnost. Pored hiperskalera, ovaj koncept postaće zanimljiv i za sve veći broj kolokatora.

Rittal svojim korisnicima nudi fleksibilnost: „Ne ograničavamo se na *Open Rack* V3 u 21-inčnoj tehnologiji. U našim VX IT ormanima takođe se primenjuje standardizovana 19-inčna tehnologija. Potpuna integracija u *Rittal* sistemsku platformu je potrebna kako bi se obezbedila IT infrastruktura potrebna za AI aplikacije u velikom obimu - od velikih *hyperscale data* centara do onih za mala preduzeća. Direktno tečno hlađenje je jedna od osnova tehnologije za AI. Naš razvoj je inspirisan našim velikim globalnim korisnicima i *Rittal*-ovim višegodišnjim iskustvom u IT i industriji. Dve decenije razvoja IT hlađenja i više od 30 godina proizvodnje rashladnih uređaja za sve, pa i najteže, industrijske uslove“, objašnjava Igor Šugar, direktor marketinga *Rittal* Srbije i dodaje: „Želimo da napravimo rezultat kako bismo dobili inovaciju dostupnu našim korisnicima - i velikim i malim - što je pre moguće“.

Rittal.com

vodom, dizajnirano za jednostavno i brzo redovno servisiranje.

Kako ovo funkcioniše? Temeljeno na modularnosti i dizajnerskim prednostima *Open Rack* V3, čiji je razvoj *Rittal* primenio i u *Open Compute Project* (OCP), sistem napajanja servera u ormanu je povezan sa centralnim dovodima i putem standardizovanih priključaka vodenog kruga. Funkcionalne jedinice, kao što su jedinica centralnog kontrolera i nekoliko *Coolant Conveying Units* (CCUs) - u zavisnosti od zahtevanih performansi - potpuno su modularni i lako se mogu ubaciti u orman. Garantuju visoku dostupnost kroz n+1 redundantni dizajn. Nadzor curenja tečnosti počinje kod svake komponente. Ovaj koncept nudi veliku korist u pogledu usluge servisa: komponente kao što su kontroleri, senzori ili *in-row* jedinice mogu se održavati tokom rada i lako zameniti putem *hot swap* sistema.

Infrastruktura direktno u ormanu

Sve više se struja, hlađenje i nadzor integrišu direktno u standardizovani orman kao osnovni temelji IT infrastrukture. Glavni pokretači ovog trenda su *hyperscale* i serverski OEM provajderi, za koje je *Rittal* glavni snabdevač IT ormana. Ubeđeni smo da će ovaj koncept uskoro postati standard za naše globalne IT ko-

Data centri i veštačka inteligencija

U svetu koji se brzo menja pod uticajem digitalne transformacije, veštačka inteligencija (AI) se nameće kao ključna tehnologija koja oblikuje budućnost

Ivan Živković, Product Application Engineer, Schneider Electric

Ovaj rastući trend prati eksplozivni razvoj *data* centara, koji predstavljaju srce AI sistema, omogućavajući obradu ogromnih količina podataka u realnom vremenu. Kao lider u oblasti energetskih rešenja i infrastrukture za *data* centre, *Schneider Electric* igra ključnu ulogu u ovoj transformaciji, pružajući inovativna rešenja koja zadovoljavaju sve veće zahteve AI tehnologije.

Novi zahtevi za AI servere i inovativna rešenja

AI serveri zahtevaju specijalizovane akceleratore, kao što su grafičke procesorske jedinice (GPU) i integrisana kola za specifične aplikacije (ASIC), poput *Google*-ovog *Tensor Processing Unit* (TPU) ili *Huawei Ascend* 910. Ovi akceleratori omogućavaju brz protok podataka i podržavaju AI učenje, računanje i zaključivanje na mnogo višem nivou efikasnosti.

Schneider Electric, kao lider u oblasti energetskih rešenja, prepoznao je ove potrebe i ponudio napredna rešenja koja zadovoljavaju specifične zahteve AI *data* centara. Njihovi proizvodi i usluge uključuju visokoefikasne sisteme za napajanje i hlađenje, kao i rešenja za praćenje i upravljanje infrastrukturom koja osiguravaju optimalne performanse i pouzdanost.

Potrošnja energije i rast AI data centara

Trenutno AI centri troše oko 4,5 GW energije globalno. Prema procenama kompanije *Schneider Electric*, do 2028. godine, potrošnja će biti između 14 i 18,7 GW. Ovaj rast je rezultat sve većih potreba za obradom podataka i učenjem AI modela.

S porastom upotrebe AI tehnologija tradicionalni metod vazdušnog hlađenja postaje neadekvatan. Kako se čipovi zagrevaju, tečno hlađenje postaje jedina održiva opcija

AI serveri rade na dva glavna tipa opterećenja: učenje i zaključivanje. Učenje uključuje razvoj početnih modela i poboljšanje tih modela na osnovu novih podataka, dok zaključivanje koristi te modele za predviđanje i donošenje odluka. Ovi procesi zahtevaju velike količine energije i odgovarajuću infrastrukturu za hlađenje i napajanje.

Tehnička rešenja za AI servere

AI serveri zahtevaju specijalizovane akceleratore, kao što su GPU-ovi i ASIC-ovi, koji omogućavaju brzu i efikasnu obradu podataka. Jedinice za obradu podataka (DPU) rade zajedno sa CPU-ima i GPU-ima kako bi poboljšali računarsku snagu i rukovanje sve složenijim obradama podataka.

Hlađenje data centara

Tečno hlađenje kao odgovor na izazove: *data* centri tradicionalno koriste vazdušno hlađenje, ali s porastom upotrebe AI tehnologija, ovaj metod postaje neadekvatan. AI obuka zahteva značajno povećanje računarskog kapaciteta, što dovodi do povećanja toplotnog dizajna procesora. Kako se čipovi zagrevaju, tečno hlađenje postaje jedina održiva opcija.

Schneider Electric nudi rešenja koja uključuju napredne sisteme hlađenja, kao što su tečno hlađenje direktno ka čipu i uranjanje u tečnost. Ova tehnologija omogućava bolje performanse i pouzdanost, smanjujući potrebu za klasičnim vazdušnim hlađenjem koje postaje neefikasno kod visokih toplotnih opterećenja u AI *data* centrima.

Schneider Electric je lider u implementaciji tečnih hlađenja, koristeći dve glavne metode: direktno na čip i uranjanje. Ova rešenja poboljšavaju pouzdanost i efikasnost, smanjujući nivo buke i potrošnju vode. *Schneider Electric*-ova rešenja uključuju sisteme za odvođenje toplote unutar servera, tipove CDU (*Cooling Distribution Unit*) i načine izbacivanja toplote napolje, čime se obezbeđuje optimalna kontrola temperature, protoka i pritiska.

Schneider Electric i NVIDIA udružuju snage za revoluciju u AI data centrima

Schneider Electric je objavio stratešku saradnju sa kompanijom NVIDIA, pionirskom kompanijom u oblasti veštačke inteligencije (AI). Ova saradnja ima za cilj revolucionarne promene infrastrukture *data* centara putem primene naprednih AI tehnologija i digitalnih blizanaca, otvarajući nove horizonte za industriju i tehnološki napredak (digitalni blizanci predstavljaju virtuelni uzorak budućih proizvoda ili usluga kroz digitalnu simulaciju procesa proizvodnje).

Kombinujući svoje bogato iskustvo u dizajnu i upravljanju *data* centrima s vrhunskim NVIDIA AI tehnologijama, *Schneider Electric* će predstaviti prve javno dostupne referentne dizajne AI centara podataka. Ovi dizajni postavljaju nove standarde za implementaciju i operativne procese u centrima podataka, omogućavajući optimizaciju resursa i energetsku efikasnost, ključne za budući razvoj veštačke inteligencije.

U prvoj fazi saradnje, *Schneider Electric* će razviti najsavremenije referentne dizajne prilagođene za NVIDIA ubrzane računarske klastere. Ovi sistemi su dizajnirani da podrže napredne primene poput inženjerske simulacije, automatizacije elektronskog dizajna, generativne AI i drugih visokointenzivnih računarskih zadataka. Fokus će biti na distribuciji velike snage i tečnom hlađenju, što je ključno za rad klastera visoke gustine.

Referentni dizajni koje će razviti *Schneider Electric* pružaju robustan okvir za implementaciju NVIDIA platformi unutar postojećih i novih centara podataka, omogućavajući skalabilnost i optimizaciju performansi. Ova saradnja će vlasnicima i operaterima *data* centara obezbediti alate za besprekornu integraciju naprednih AI rešenja, poboljšavajući efikasnost i pouzdanost tokom celog životnog ciklusa.

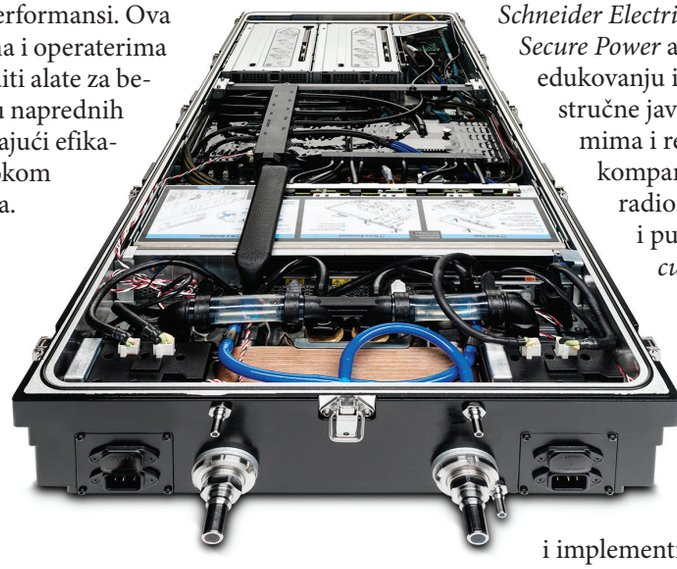
Uz to, AVEVA, podružnica *Schneider Electric*-a, povezaće svoju digitalnu platformu blizanca s NVIDIA *Omniverse*-om, omogućavajući virtuelnu simulaciju i kolaboraciju. Ova integracija će ubrzati dizajn i implementaciju složenih sistema, smanjujući vreme do tržišta i troškove.

Schneider Electric i NVIDIA zajedno istražuju nove primene u raznim industrijama, pokrećući pozitivne promene i oblikujući budućnost tehnologije. Ova saradnja obećava da će *data* centri sutrašnjice biti energetski efikasniji, ekonomski isplativiji i tehnološki napredniji, čime se otvara nova era u primeni veštačke inteligencije.

Saradnja kompanija Schneider Electric i NVIDIA u oblasti veštačke inteligencije ima za cilj revolucionarne promene infrastrukture data centara putem primene naprednih AI tehnologija i digitalnih blizanaca

Projekcija rasta i izazovi za budućnost

S porastom upotrebe AI, potražnja za AI *data* centrima eksponencijalno raste. Ovo donosi izazove u pogledu efikasnog hlađenja i upravljanja visokom gustinom snage koju generišu AI serveri i GPU-ovi. *Schneider Electric* predviđa značajan rast u ovoj oblasti i nudi rešenja koja omogućavaju optimizaciju performansi i energetsku efikasnost.



Schneider Electric-ov tim *Secure Power* aktivno radi na edukovanju i upoznavanju stručne javnosti s problemima i rešenjima koje kompanija nudi. Kroz radionice, seminare i publikacije, *Secure Power* tim pruža ključne informacije i obuku koja pomaže stručnjacima da razumeju nove tehnologije i implementiraju ih na optimalan način.

Zaključak

U svetu gde veštačka inteligencija postaje sve prisutnija, *data* centri su ključni za podršku ovog rasta. *Schneider Electric*, sa svojim inovativnim rešenjima i stručnim timom, igra ključnu ulogu u ovoj oblasti. Njihovi proizvodi i usluge ne samo da zadovoljavaju trenutne potrebe već i postavljaju temelje za budući razvoj i rast AI tehnologija.

Schneider Electric se pozicionirao kao lider u oblasti energetske efikasnosti i infrastrukture za *data* centre, pružajući rešenja koja omogućavaju visoke performanse, pouzdanost i održivost. Sa rastom AI industrije, uloga *Schneider Electric*-a postaće još značajnija, obezbeđujući da *data* centri budu spremni za izazove budućnosti.

se.com/rs

PC PRESS

Računari i Galaksija ponovo u vašoj kući

Povodom jubileja, 40 godina od premijere,
PC Press je objavio reprint izdanja
Računara i novu verziju računara Galaksija

Računari u vašoj kući, nekad i sad

Monografsko izdanje legendarnog časopisa iz 1984. godine. Komplet sadrži digitalizovani reprint originilanog izdanja i novu publikaciju na 48 strana sa uputstvom za samogradnju nove verzije računara Galaksija iz 2024. godine.

Galaksija 2024

Voja Antonić je pripremio novu verziju Galaksije potpuno kompatibilnu sa originalom, ali prilagođenu današnjem vremenu! Nova Galaksija se priključuje na monitor, napaja punjačem za mobilne, a programi se upisuju na flash memoriju.

Poručite odmah
www.racunari.com

Možete li zamenom starog UPS uređaja za novi da uštedite novac?

Novi UPS uređaji imaju tehnologiju koja znatno povećava energetsku efikasnost, odnosno smanjuje potrošnju električne energije, čime će računi biti niži

Nataša Kovačević

Zastarela oprema jedan je od vodećih uzroka zastoja u radu *data* centara, što utiče na ukupnu produktivnost i efikasnost. Takođe, sprečava korisnike da ispune trenutne i buduće poslovne zadatke i obaveze. Tabela ispod prikazuje uslove koji ukazuju da je UPS blizu kraja korišćenja za datu aplikaciju.

Zamena UPS uređaja uključuje: evaluaciju postojećeg sistema i preporuku za novi uređaj, nabavku, isporuku i puštanje u rad novog UPS uređaja, uz ostale usluge: produženu garanciju, odnošenje i reciklažu starog UPS-a, preradu ili zamenu električnih instalacija, kao i mogućnost potpisivanja novih servisnih ugovora, koji imaju povoljnije uslove. Postoje tri glavne faze u životnom ciklusu UPS uređaja koje su prikazane na slici:

Faza komercijalizacije

Faza komercijalizacije počinje kada se određeni model UPS uređaja lansira na tržište i traje sve do njegovog povlačenja s tržišta. U ovoj fazi, i proizvod i usluge su u potpunosti dostupni.

Faza usluga

Faza usluga počinje s povlačenjem proizvoda s tržišta, kada određeni model UPS uređaja više nije dostupan za prodaju, nego je zamenjen novom tehnologijom. U ovoj fazi podrška proizvođača i rezervni delovi se i dalje proizvode i mogu se nabaviti, pa su dostupne samo usluge, ali ne i sam proizvod. Kod svih ozbiljnih proizvođača UPS uređaja faza usluga traje 10 godina.

Faza kraja radnog veka

Faza kraja radnog veka je faza kada ni proizvod, ni usluge za taj model UPS-a nisu više dostupni, tako da je kontinuitet rada u realnoj opasnosti. Ako se proizvod pokvari, rezervni delovi i podrška neće biti dostupni. Tada jedino ostaje zamena novim UPS uređajem.

Prednosti zamene starog UPS uređaja novim

Kada se UPS nalazi u fazi usluga, cene rezervnih delova i usluga se znatno povećavaju u odnosu kada se UPS nalazi u fazi komercijalizacije (pogledajte sliku). Tako da se nabavkom novog UPS uređaja smanjuju troškovi održavanja.

Pored smanjenja troškova održavanja, novi UPS uređaji smanjuju i troškove potrošnje električne energije, jer su energetski efikasniji.

Pored uštede novca, prednosti da stari UPS zamenite novim su: smanjenje rizika od neočekivanog zastoja, dostupnost rezervnih delova, kao i pristup održavanju i dijagnostici 24/7 putem mobilnog uređaja.

Kada se menja UPS u *data* centru, preporuka stručnjaka je da bi uvek trebalo nešto poboljšati: ili da sistem ima veću efikasnost, ili da postane pouzdaniji, npr. ako je bio u N sistemu, da se nabavi redundantan sistem, odnosno [N+1] konfiguracija, ili da se pređe na modularno rešenje, ili da se malo povećaju snaga ili autonomija.

Ako želite da zamenite svoj UPS novim ili ukoliko nabavljate novi UPS, slobodno nas pozovite.

konvereks.rs

Situacija	Opis
Ne može da ispuni kritične zahteve	Ako UPS ne može da zadovolji trenutne ili buduće zahteve, na primer ne može da podrži celokupno IT opterećenje, ili nema odgovarajući nivo pouzdanosti, ili ima nedovoljnu autonomiju, onda je na „kraju životnog veka", barem za tu aplikaciju.
Kada prestane podrška proizvođača	Podrška proizvođača prestaje 10 godina nakon što je model povučen s tržišta. Nedostatak podrške čini rutinsko održavanje i servisiranje nepraktičnim, ako ne i nemogućim.
Kada su nedostupni rezervni delovi	Kada rezervni delovi postanu nedostupni, malo je opcija za održavanje/servisiranje UPS uređaja.
Skupo održavanje	Kako oprema stari, potreba za održavanjem se povećava. Moguće je da troškovi i rizici održavanja prevaziđu troškove i koristi (kapacitet, efikasnost i pouzdanost) ugradnje novog sistema.

Izazovi savremenih data centara

Savremeni data centri se suočavaju s mnoštvom izazova. Brz napredak u oblasti veštačke inteligencije (AI) i sve veća potražnja za superbrzom obradom podataka traže dodatne resurse, a Supermicro SuperKlaster skalabilne jedinice predstavljaju moćno rešenje

Dok organizacije širom sveta nastoje da zadovolje rastuće zahteve za obradom podataka, *data* centri moraju stalno da se razvijaju. Ova evolucija nije samo pitanje skaliranja već i integrisanja najsavremenijih tehnologija kako bi se isporučila sveobuhvatna rešenja.

Inovativna hardverska rešenja

Supermicro SuperKlaster skalabilne jedinice predstavljaju značajan iskorak u hardverskim rešenjima dizajniranim za neprevaziđene performanse i skalabilnost. Karakteriše ih konfiguracija s devet *rack*-ova, a opremljene su sa 32 NVIDIA HGX H100 grafička procesora po *rack*-u. Ova postavka donosi 256 NVIDIA H100 GPU skalabilnih jedinica, pružajući izuzetnu procesorsku snagu.

Klasteri imaju široke AI mogućnosti i mrežu vrhunskih performansi, prilagođenu zahtevnim računarskim zadacima. Softverski ekosistem, uključujući NVIDIA AI *Enterprise*, SLURM i *Kubernetes* obezbeđuje fleksibilnost i besprekornu integraciju s mnogim rešenjima, postavljajući *Supermicro* hardver kao lidera u savremenoj obradi podataka.

Proizvodni kapaciteti u SAD

Proizvodni kapaciteti kompanije *Supermicro* u Sjedinjenim Američkim državama predstavljaju dokaz posvećenosti kvalitetu i proizvodnji vrhunske opreme. Pogon ima kapacitet za istovremeno testiranje

SUPERMIKRO SUPERMICRO CodeCell

CPU i GPU su dizajnirani tako da pruže poboljšane performanse uz nižu potrošnju energije

više od 400 *rack*-ova, proizvodnju 600.000 sistema godišnje i sklapanje 5.000 rack-ova mesečno. Ova robusna infrastruktura podržava mrežna testiranja visokih performansi i nudi raznovrsne opcije napajanja, dokazujući da je kompanija *Supermicro* sposobna da efikasno i precizno zadovolji različite potrebe globalnih *data* centara.

Pristup kompanije *Supermicro* u dizajnu rešenja je holistički i konsultativan i obuhvata dizajn, sklapanje, testiranje, implementaciju i kontinuiranu podršku. Ova sveobuhvatna strategija osigurava da organizacije mogu pristupiti modernoj AI infrastrukturi prilagođenoj njihovim specifičnim zahtevima. Tim iskusnih stručnjaka kontroliše svaki korak, od koncepta do implementacije, osiguravajući da rešenja, ne samo da zadovoljavaju već i prevazilaze potrebe organizacije.

Prilagođavanje promenljivim radnim opterećenjima

Digitalna transformacija menja industrije, a IT odeljenja su na čelu ove promene, zadužena za poboljšanje performansi i sposobnosti unutar često ograničenih budžeta. Podrška raznovrsnim radnim opterećenjima, kao što su analitičke platforme, AI, mašinsko učenje i različita naučna istraživanja zahteva robusne, aplikaciono optimizovane servere i sisteme za skladištenje. Ovi sistemi moraju pružati visoke performanse uz optimizaciju troškova, a rešenja kompanije *Supermicro* ispunjavaju oba ova zahteva, omogućavajući IT odeljenjima da efikasno zadovolje promenljive zahteve.

Planiranje osvežavanja hardvera

Efikasno planiranje osvežavanja hardvera je ključno za održavanje konkurentske prednosti. Ovaj proces počinje suštinskim razumevanjem korporativnih ciljeva i IT zahteva. Revizija postojeće infrastrukture može pomoći u evaluaciji potrebnih performansi, kompatibilnosti softvera i potencijala za ponovnu upotrebu zastarelog hardvera. Pravilno planiranje osigurava besprekornu integraciju novih tehnologija, maksimizirajući

dobitke u performansama i izbegavajući prekide. Ovaj strateški pristup je ključan za organizacije koje žele da opstanu u tehnološkom okruženju koje se brzo razvija.

Korišćenje novih tehnologija, kao što su najnoviji API-ji i napredne karakteristike CPU-ova i GPU-ova, može znatno poboljšati performanse i sigurnost. Razumevanje ovih inovacija i modifikacija aplikacija kako bi se iskoristile njihove mogućnosti ključno je za uspešno osvežavanje *data* centra. Rano testiranje i validacija novih tehnologija od suštinskog su značaja, jer osiguravaju glatku tranziciju i optimalne performanse. Posvećenost kompanije *Supermicro* inkorporiranju ovih inovacija u svoje proizvode omogućava organizacijama da ostanu na čelu tehnološke revolucije.

Supermicro X13 linija

Supermicro X13 porodica proizvoda, koje pokreću četvrta i peta generacija *Intel® Xeon® Scalable* procesora, nude niz tehnoloških inovacija prilagođenih različitim radnim opterećenjima. Bilo da se radi o GPU serverima, serverima za skladištenje ili multiprocesorskim sistemima, X13 linija proizvoda ističe posvećenost kompanije *Supermicro* pružanju najmodernijih rešenja. Ovi proizvodi su dizajnirani da maksimiziraju performanse i efikasnost, zadovoljavajući različite potrebe savremenih *data* centara i osiguravajući da ostanu konkurentni u svetu vođenom tehnologijom.

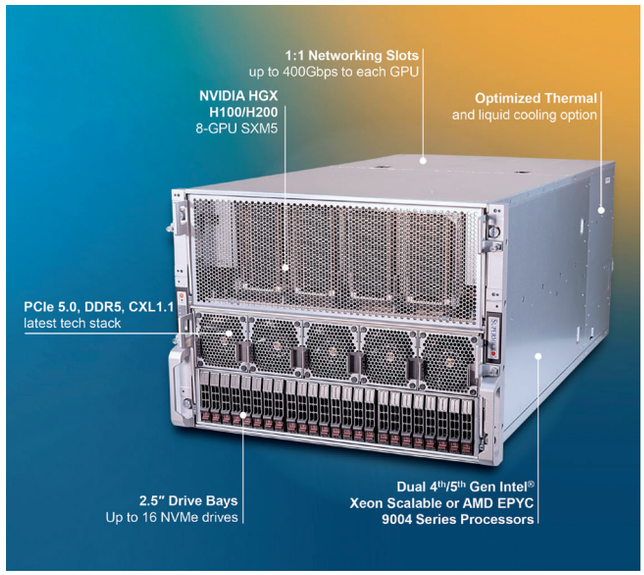
Inicijative za zelenu računarsku tehnologiju

Usvajanje novijeg hardvera često se usklađuje sa ekološkim, „zelenijim“ praksama. Najnoviji CPU-ovi i GPU-ovi su dizajnirani da pruže poboljšane performanse uz nižu potrošnju energije. Integracijom ovih energetski efikasnih sistema, *data* centri mogu smanjiti potrošnju električne energije uz održavanje ili čak poboljšanje ukupnih performansi. Ovo ne samo da pomaže u smanjenju operativnih troškova već i doprinosi održivosti životne sredine.

Pored operativne efikasnosti, *data* centri moraju razmatrati svoj ukupni ekološki otisak. Inovativni koncepti, kao što su vodeno hlađenje i arhitekture za uštedu energije, igraju ključnu ulogu u smanjenju potrošnje energije i minimizaciji elektronskog otpada. Dizajn sistema s neintegrisanom arhitekturom omogućava laku zamenu komponenti i tako postiže dugoročnu održivost. Ove ekološki svesne strategije su integralne za moderni dizajn *data* centara – tehnološki napredak ne sme ići na štetu planete.

Totalna IT rešenja i napredna Klaster rešenja

Totalna IT rešenja kompanije *Supermicro* pružaju organizacijama unapred testirane i validirane kombinacije hardvera i softvera prilagođene za rešavanje specifičnih izazova. Njihova stručnost osigurava testiranje u proizvodnji na nivou više rack-ova, rezultirajući potpuno operativnim *Klaster* rešenjima koja pojednostavljuju implementaciju i optimizuju performanse. Ovaj nivo integracije i validacije pomaže organizacijama da brže i efikasnije implementiraju nove tehnologije, smanjujući zastoje i povećavajući produktivnost.



Vrhunska optimizacija i moderna arhitektura

Dok se kompanije suočavaju sa sve kompleksnijom organizacijom savremenih *data* centara, potreba za strateškim ciklusima osvežavanja hardvera postaje sve očiglednija. Prihvatanjem ranog pristupa najsavremenijim tehnologijama, korišćenjem naprednih rešenja kompanije *Supermicro* i davanjem prioriteta ekološkoj održivosti, organizacije mogu osigurati glatku i efikasnu transformaciju *data* centara. Na taj način, organizacije mogu uskladiti kapacitete svojih *data* centara s poslovnim ciljevima, podstičući inovacije i održavajući konkurentsku prednost.

Klaster rešenja kompanije Supermicro

Na našem tržištu, naprednim *Supermicro* rešenjima se već više decenija uspešno bavi kompanija *Supermikro* iz Beograda kao prvi distributer i sistem integrator sa ovih prostora. U portfoliju proizvoda i usluga možete naći sve ono što kompanija *Supermicro* radi globalno. Raspoložive su sve vrste servera, dizajniranje serverskih rešenja, rešenja za skladištenje i obradu podataka, usluge brzog servisiranja kao i napredne podrške.

supermikro.rs

Prednosti mikro data centara u teškim industrijskim i komercijalnim okruženjima

Sve veća potražnja za IT resursima prouzrokuje sve više edge instalacija, često i na vrlo nepogodnim lokacijama. Vertiv™ SmartCabinet™ ID je idealno rešenje za zahtevne primene na edge lokacijama

Godinama su nam medijski stručnjaci govorili da dolazi Industrija 4.0., a sad već imamo i Industrijski Internet stvari (IIoT). Proizvođači koriste procese vođene IIoT-om, poput automatizacije robotskih procesa, kako bi povećali obim proizvodnje i kvalitet. IIoT takođe optimizuje druge operacije u fabrikama i mrežama, omogućavajući daljinsko praćenje, prediktivno održavanje opreme, logističke i procese lanca snabdevanja i još mnogo toga. Tako IIoT stvara krug vrednosti koji koristi i kompanijama i partnerima.

Ostale industrije takođe koriste 5G, senzore, *edge* mogućnosti, računarsku opremu i daljinski nadzor kako bi omogućile nove trendove primene IIoT-a, donoseći veću preciznost B2B procesima. Proširena stvarnost (AR) vodi radnike kroz obuku i popravke na radnom mestu. Nosivi uređaji, senzori, kamere i signali za navođenje pomažu u nadzoru i poboljšanju sigurnosti na radnom mestu. IIoT se može koristiti za automatsko dopunjavanje sirovina i proizvoda, autentifikaciju robe dok putuje kroz lanac snabdevanja te upravljanje imovinom i flotama. Industrije kao što su automobilska industrija, potrošački pakovani proizvodi i farmaceutski proizvodi mogu imati koristi od primene IIoT-a.

Stoga nije ni čudo što se predviđa da će se tržište IIoT-a oporaviti od usporavanja izazvanog epidemijom COVID-19 i porasti na 263,4 milijarde dolara do 2027. Pametna fabrika budućnosti seli se u sadašnjost.

Ubrzavanje i upravljanje edge implementacijama u nekontrolisanim okruženjima jednostavnije je uz SmartCabinet™ ID. Ovo all-in-one rešenje zadovoljava potrebe tima za zaštitom, efikasnim hlađenjem i pouzdanim rezervnim napajanjem

Tehnološka oprema neophodna za rad u teškim i izazovnim okruženjima

Pred nama je izazov. Računarstvo u oblaku (*cloud computing*) jednostavno ne može da obradi ogromna radna opterećenja podataka. Da bi se omogućila obrada s niskom latencijom i visokim propusnim opsegom, IIoT zahteva da *data* centri, IT timovi i timovi za objekte postave tehnologiju na novu lokaciju koja nije dizajnirana i izgrađena kao sobe ili kabineti za obradu podataka. Dok bi serveri, storidži i drugi uređaji radili u visokokontrolisanim okruženjima *data* centara, sada se postavljaju na prometne spratove bolnica i zdravstvenih centara, na proizvodnim mestima, u pomoćnim prostorijama maloprodajnih trgovina i slično.

Ova komercijalna i industrijska okruženja nisu izgrađena i projektovana tako da budu sobe ili kabineti za obradu podataka. Postavljanje IT opreme u tim okruženjima može dovesti do potencijalne izloženosti prašini, promenama temperature i vlažnosti, što dovodi do neispravnog rada ili kvarova. Na određenim lokacijama, kao što su proizvodna mesta, izloženost tečnostima, kao što su curenje iz nadzemnih cevi ili kanalizacionih vodova, takođe može predstavljati problem. Nadalje, obično nije poželjno niti praktično naknadno opremiti te prostore ekološkim kontrolama i hlađenjem koje tehnologija zahteva za efikasan rad.

Mikro data centri nude uverljivo rešenje za industrijske edge implementacije

Gde god se tehnologija koristi, IT timovi žele da je zaštite od uslova sredine i fizičke štete. Takođe, žele pomno da prate efikasnost tehnologije kako bi pružili visoku dostupnost koju zahtevaju sve složeniji digitalni procesi i korisnička iskustva. Na sreću, postoji sigurno rešenje koje nudi aplikaciju neutralnu prema prostoriji: mikro *data* centri za zahtevna okruženja.

Mikro data centar: pravo rešenje

Mikro *data* centri integrišu sve kritične elemente konvencionalnog *data* centra u kompaktnu celinu, omogućavajući im efikasan rad u različitim

okruženjima. Svaka jedinica služi kao *all-in-one* rešenje koje uključuje napajanje, hlađenje, serverske *rack* ormare i softver za upravljanje i nadgledanje.

Mikro *data* centar rešenja u potpunosti zaokružuju opremu u inteligentne ormare koji imaju IP54 ocenu, pružajući idealne unutrašnje radne uslove i temperature za zaštitu vredne i osetljive IT opreme. Integrisano hlađenje i izbacivanje spoljne toplote rade zajedno kako bi zaštitili tehnologiju i poslovne procese koje omogućavaju. To je važno jer ovi tehnološki ormari mogu biti postavljeni uz tešku operativnu tehnologiju koja neprekidno radi i podiže ambijentalnu temperaturu okolnih područja.

Zbog svoje kompaktne veličine, mikro *data* centar omogućava brzu implementaciju u unutrašnjim i spoljnim prostorima, uključujući udaljene lokacije. To ga čini idealnim rešenjem za podružnicu ili za privremenu upotrebu u visokorizičnim zonama gde bi tradicionalni *data* centri bili nepraktični.

Poboljšano praćenje i nadzor

Mikro *data* centri omogućavaju lokalni i daljinski nadzor. Senzori pružaju stalna ažuriranja o temperaturi, vlažnosti, protoku vazduha, detekciji poplave i još mnogo toga, omogućavajući timovima da odmah preduzmu korektivne mere ako se pojavi problem. Pomoćni ventilator za hitne slučajeve može pružiti dodatno osiguranje, obezbeđujući pravilan protok vazduha i izbegavajući pregrevanje ako rashladni sistemi zakažu.

Osiguravanje neprekidnog rada tehnologije

Osim nadzora okolnih uslova, timovi mogu osigurati neprekidan rad tehnologije pomoću integrisane distribucije energije i mogućnostima rezervnog napajanja. Jedinice za distribuciju električne energije u serverskom ormaru (rPDU) i neprekidni izvori napajanja (UPS) nadgledaju dostupnost sistema i osiguravaju rezervno napajanje u slučaju problema, sprečavajući zastoje.

Mere fizičke sigurnosti

Konačno, za mikro *data* centre treba osigurati i snažnu fizičku kontrolu. Inteligentne brave na prednjim i zadnjim vratima ograničavaju pristup ovlašćenim korisnicima, dok senzori na vratima mogu odmah upozoriti timove na sve pokušaje pristupa opremi.

Vertiv™ SmartCabinet™ ID je idealno rešenje za zahtevne primene na edge lokacijama.

Računarstvo u oblaku (cloud computing) jednostavno ne može da obradi ogromna radna opterećenja podataka. Da bi se omogućila obrada s niskom latencijom i visokim propusnim opsegom, IIoT zahteva da data centri, IT timovi i timovi za objekte postave tehnologiju na novu lokaciju koja nije dizajnirana i izgrađena kao sobe ili kabineti za obradu podataka

Vertiv™ SmartCabinet™ ID pruža sve te mogućnosti - nadzor uslova okoline, integrisano hlađenje, nadzor napajanja, pomoćno napajanje zahvaljujući *Vertiv™ Liebert®* GXT5 UPS-u i fizičkim kontrolama. *SmartCabinet™* ID potpuno je zatvoren, s IP54 ocenom i pruža 3,5 ili 7 kW potpuno integrisanog hlađenja, štiteći vrednu računarsku opremu gde god je postavljena.

Osim toga, *SmartCabinet* ID isporučuje se u malom formatu koji se lako postavlja. Umesto izgradnje mrežnih ormara ili postavljanja glomaznih *rack* ormara tamo gde im nije mesto, timovi mogu da implementiraju *SmartCabinet* ID u ograničenim, skučenim prostorima. Takođe, mogu iskoristiti prednost rešenja s hlađenjem koje ne zauzima prostor (*zero-U cooling*) kako bi u svaki ormar smestili više računarske opreme, napajajući više procesa i povećavajući povrat ulaganja (ROI).

Na kraju, *Vertiv™ SmartCabinet™* ID zadovoljava želju timova za brzim plasmanom na tržište s rešenjem koje se može instalirati za samo jedan dan. Uz globalnu proizvodnju i dostupnost, problemi u lancu snabdevanja nisu zabrinjavajući.

Ubrzavanje i upravljanje *edge* implementacijama u nekontrolisanim okruženjima jednostavnije je uz *SmartCabinet™* ID. Ovo *all-in-one* rešenje zadovoljava potrebe tima za zaštitom, efikasnim hlađenjem i pouzdanim rezervnim napajanjem. Njegov kompaktni dizajn, modularnost i brza implementacija nude značajnu prednost, čineći ovo svestrano rešenje prikladnim za *edge* okruženja koja zahtevaju zaštitu od teških uslova.

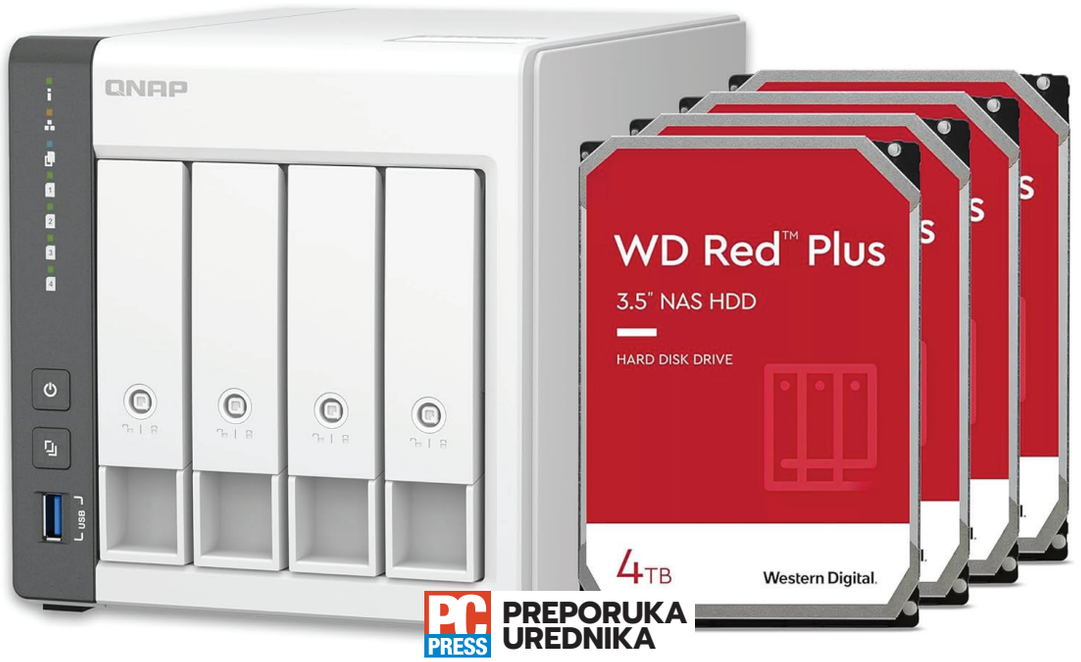
Uz to, implementacija *SmartCabinet™* ID-ja traje danima umesto mesecima. Nemojte uzalud trošiti svoj proračun na izgradnju posebne prostorije za zaštitu vašeg IT-ja, investirajte inteligentno u *SmartCabinet* ID.

Saznajte više o *Vertiv™* SmartCabinet™ ID na *Vertiv.com* ili kontaktirajte s našim odeljenjem prodaje u Zagrebu na *croatia.hello@Vertiv.com*.

NAS na AI steroidima

QNAP TS-433 je osmišljen kao budžetski orijentisan NAS za sve koji žele multimedijalni centar, privatni cloud, video-nadzor i malo veštačke inteligencije za prepoznavanje lica i slične zadatke

Mirko Topalović



Punih 14 godina *Google* nudi besplatne servise svojim korisnicima, i tako je više od pola planete Zemlje „navučeno" na *Gmail*, *Google Photos*, *Drive*, *YouTube* i druge zgodne aplikacije. Od 2014. godine *YouTube* je uveo *Premium* servis za sve koji ne žele da gledaju reklame, a četiri godine kasnije i *Google One* servis za sve one koji su popunili svoj besplatan prostor na ostalim servisima. I dok *YouTube Premium* ne možete tako lako da zaobiđete, *cloud* pretplatu i servise možete. NAS uređaji vam nude fleksibilnost privatnih *cloud* servisa koji mogu da rade gotovo sve što i popularna *cloud* rešenja, s tom razlikom što se svi podaci nalaze kod vas, i što ne morate da plaćate pretplatu.

Pored privatnog *cloud* rešenja, koje je samo jedno od mogućnosti NAS uređaja, tu su i servisi poput multimedijalnog centra, video-nadzora, e-*mail* klijenta, *download* klijenta i još mnogo toga. Količinu raspoloživog prostora kontrolišete sami dodavanjem hard ili SSD diskova u četiri raspoložive fioke, a pristup je moguć, kako žično i bežično u lokalnoj mreži, tako i sa udaljene lokacije, preko mobilnog telefona ili bilo kog drugog uređaja.

S širokim dijapazonom NAS uređaja, QNAP je kompanija koja nudi rešenja za najrazličitije potrebe, klasifikovane u različite cenovne rangove. Model koji vam danas predstavljamo, QNAP TS-433-4G, predstavlja moćnu ulaznicu u QNAP svet, s modernim hardverskim rešenjima, koja će vam omogućiti da idete u koraku sa savremenim trendovima. Četiri slota omogućavaju najrazličitije konfiguracije skladišnog sistema – od JBOD i *Single* preko osnovnih RAID 0 i 1, do naprednih RAID 5, 6 i 10 kombinacija.

Moderni 64-bitni ARM procesor radi na 2 GHz i omogućava 4K video-reprodukciju (ali ne i transkoding), video-nadzor (dobijate dve licence za kamere za QVR *Elite*) i sve ostale servise QNAP ekosistema. Tu su prostrana 4 GB RAM-a i isto toliko *flash* memorije, ali i lepa iznenađenja poput dva LAN porta, od kojih jedan podržava 2,5 Gbit specifikaciju. Iako su 2,5G LAN portovi tek odnedavno počeli da se pojavljuju na matičnim pločama i ruterima, ovo je svakako zgodna stavka koja će pojačati brzine prenosa u lokalu s podržanim uređajima. Ako ne danas, onda sigurno za koju godinu.

Iako se mnogi mršte na pomisao ARM procesora, 64-bitni *Cortex* A55 ima četiri jezgra, *Mali*-G52 grafiku, NPU

QNAP TS-433-4G	
Procesor	ARM 4-core Cortex-A55 2 GHz 64-bit
RAM	4 GB integrisano (nije proširivo)
GPU	Mali-G52
Flash memorija	4 GB integrisano (nije proširivo)
Broj HDD/SSD slotova	4×3,5" SATA 6 Gbps
RJ-45 LAN portovi	1×1 Gbps + 1×2,5 Gbps
USB 2.0 portovi	2 Type A
USB 3.2 Gen 1 portovi	1 Type A
Operativni sistem	QTS 5.1.3
Podržani režimi rada	JBOD, Single, RAID 0, 1, 5, 6, 10
SSD keširanje	ne
Interni fajl sistem	EXT4
Fajl sistem eksternih uređaja	EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Hlađenje sistema	1×120 mm ventilator
Dimenzije	165×160.2×220.5 mm
Masa	3,5 kg (bez diskova)
Napajanje	65 W adapter
Potrošnja pri radu	22,54 W
Cena	69.999,98 dinara

jedinice i skoro upola manju potrošnju od rešenja kao što je *Intel Celeron*. To znači da će sa četiri diska potrošnja u radu u proseku biti malo preko 20 W, što donosi uštedu na računu za struju, posebno na duge staze.

Uređaj je dizajniran u klasičnom QNAP minimalističkom stilu, zamišljen kao rešenje koje se neprimetno uklapa u bilo koji prostor, a opet nudi i četiri HDD/SSD slota, dva LAN porta, tri USB-a i sve to u elegantnom tihom kućištu koje malo troši i ne zagreva se previše. Ograničenja TS-433-4G modela su fiksna količina RAM-a i *flash* memorije, nedostatak SSD keširanja i HDMI porta. Kao neko ko aktivno koristi NAS uređaje, HDMI konektor je lep dodatak, ali ako već imate brzu mrežu s povezanim uređajima, HDMI često bude čist višak, dok su proširenje i SSD keširanje ostavljeni za skuplje modele.

QNAP je nedavno ažurirao svoje mobilne aplikacije za kontrolu uređaja, pristup fajlovima i *download*, značajno olakšavši procese poput deljenja podataka, ali i *backup* fotografija i video-snimaka s telefona, omogućavajući vam da se odreknete neke od pretplata koje redovno plaćate. Primera radi, ako plaćate neku od premijum *cloud* pretplata kao što je *Google One* od 2 TB, za pet godina plaćanja dolazite do cene jednog TS-433 uređaja, koji može sve to, i još mnogo više. Dodajte tu i dve licence za kamere za video-nadzor, VM platformu, aplikacije za strimovanje i multimediju, i jasno vam je da je NAS moćan uređaj koji nudi mnogo više od personalnog *cloud* rešenja.

QNAP je nedavno ažurirao svoje mobilne aplikacije za kontrolu uređaja, pristup fajlovima i download, značajno olakšavši proces deljenja podataka

Kao bonus, TS-433 ima CPU s NPU mogućnostima, što znači da ćete imati znatno bolje performanse u poslovima kao što je prepoznavanje lica i sličnim primenama koje se mogu osloniti na mašinsko učenje i veštačku inteligenciju. Tu je i moderna verzija QTS operativnog sistema u verziji 5.1.6 koja nudi odlično *desktop* i mobilno okruženje za laku navigaciju i podešavanja sistema iz bilo kog *browser*-a.

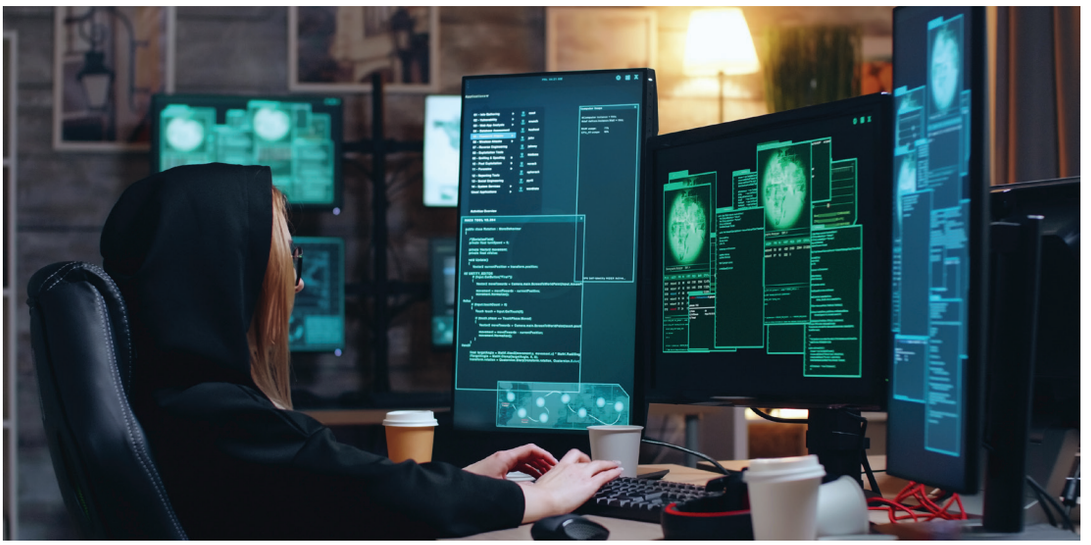
QNAP TS-433 je dobro i pristupačno rešenje koje će podmiriti sve vaše potrebe i otvoriti vrata ka mnogim drugim mogućnostima, čiji ćete značaj tek sa vremenom shvatiti.

www.mikroprinc.com

Upravljanje sajberbezbednošću

Stara izreka koja kaže da je lanac jak onoliko koliko je jaka njegova najslabija karika, predstavlja jedan od kamena temeljaca u sajberbezbednosti. Napretkom tehnologije novih „karika" je sve više, stare redovno treba proveravati, a poslovni i tehnički zahtevi koji se stavljaju pred „lanac bezbednosti" sve su brojniji i kompleksniji

Kristijan Lazić



Među IT stručnjacima često se čuje rečenica da postoje IT sistemi koji su pretrpeli sajbernapad i oni za koje se još uvek ne zna da su bili (ili su još uvek!) meta napada. Iako je reč o šali koja nije sasvim tačna, poruka je jasna – pitanje nije da li će se bezbednosna pretnja pojaviti, već kada. A kada se pojavi, na putu joj stoje samo dva bedema – maksimalni negativni uticaj koji može ostvariti na IT sistem (ili njegov deo) i verovatnoća da u toj nameri uspe. Jednostavnije rečeno, dobra IT bezbednost predstavlja „računicu" da branjeni IT sistem napadaču ne bude isplativ, tj. da napor uložen u napad rezultira manje vrednom „nagradom".

Ukoliko posmatramo sajbernapade kroz prizmu finansijske matematike, a ne kao zabavu i dokazivanje naprednih tehničkih veština, zadaci odbrane IT sistema postaju u isto vreme i laki i teški. Lakši deo jednačine čini to što postoji „bezbroj" proverenih načina i metoda koji nas mogu voditi putem uspostavljanja adekvatnog digitalnog imuniteta, a teži, da put uspostavljanja i upravljanja sajberbezbednošću predstavlja kompleksan zadatak na kome u mnogo koraka možemo napraviti grešku i (nenamerno) stvoriti onu „slabu kariku" s početka teksta.

Odozdo naviše?

Jedna od najčešćih grešaka koje u praksi olakšavaju aktivnosti napadačima jeste uspostavljanje sajberbezbednosti po principu „odozdo naviše", odnosno stvaranje bezbednosti od implementacije određene tehnologije (npr. određenog sistema za detekciju zlonamernog koda, zaštitu mreže od spoljnih napada i slično), koji se „širi" na ostale (tehničke) elemente IT okruženja – *data* centar, *cloud* servise, aplikacije, radne stanice, pa čak i davanjem prednosti zaposlenima sa specifičnim tehnološkim znanjima. Iako je ovakav način kreiranja zaštitnih slojeva bolji od neplanskog i reaktivnog pristupa („rešavaću problem kad se on desi"), održavanje i nadgradnja s vremenom postaju manje efikasni, manje fleksibilni i posledično – skuplji.

Dobra IT bezbednost predstavlja „računicu" da branjeni IT sistem napadaču ne bude isplativ, tj. da napor uložen u napad rezultira manje vrednom „nagradom"

Teži, sporiji, ali dugoročno bolji put izgradnje sajberbezbednosti jeste onaj gde odgovori na dva najvažnija pitanja od kojih treba krenuti – šta želimo da zaštitimo i koliko temeljno – određuju pristup, metodologiju i sve naknadne konkretne korake (princip „odozgo naniže"). Iako deluje paradoksalno, drugi pristup je dugoročno jeftiniji. Ne treba nikada zaboraviti da je dovoljan samo jedan (ne)uspešan napad, pa da organizacija od lidera na tržištu postane zaboravljena firma.

U praksi su ipak najčešće situacije gde put podizanja nivoa sajberbezbednosti počinje „iz sredine" – neke tehnologije i procesi zaštite su već prisutni, ali mnogo detalja još nedostaje, pre svega u delu saradnje sajberbezbednosti s poslovnim procesima i misijom organizacije. Logičan naredni

korak u realnost je izbor odgovarajućeg okvira za upravljanje sajberbezbednošću i njegova implementacija.

Okviri za upravljanje sajberbezbednošću

Okviri za upravljanje sajberbezbednošću predstavljaju skupove dokumenata koji opisuju smernice i standarde za upravljanje rizikom od sajberbezbednosti. Reč „okvir" se odnosi na najbolju praksu koju treba uspostaviti u svakom aspektu IT sistema, a ne samo tehničkom, na način da zajedno čine celinu. Dobra vest je da danas postoji više desetina robusnih, proverenih i u praksi prihvaćenih okvira, po čijim smernicama možete urediti sve aspekte bezbednosti. Ne tako dobra vest je da nije uvek jednostavno odabrati onaj koji će najbolje odgovarati potrebama vaše organizacije.

Prva u nizu odluka koji slede je izbor tipa okvira; ukoliko ste na samom početku, bez iskustva u implementaciji i upravljanju, prirodan korak su kontrolni okviri. Reč je o dokumentima koji u sebi sadrže najviše „tehničkog jezika", i kao takvi, lakše i jednostavnije se usvajaju od zaposlenih u IT sektoru, što je jedan od najvažnijih dugoročnih faktora uspeha. Kontrolni okviri sadrže osnovnu listu bezbednosnih kontrola, smernice za procenu trenutnog stanja infrastrukture, aplikacija, mreža i druge tehnologije i imaju za cilj da uspostave osnovnu strategiju sajberbezbednosti organizacije. Prioritet je na pravilnoj implementaciji bezbednosnih tehnologija i kontrola, kao i ojačavanju osnovnih linija odbrane, ne ostavljajući prostora da se zaboravi neki važan element i na taj način otvori „bezbednosna rupa".

Drugoj grupi pripadaju programski okviri, koji za cilj imaju unapređenje osnovnih bezbednosnih elemenata, pomažući organizacijama da izrade, uspostave, implementiraju i redovno unapređuju sveobuhvatan program sajberbezbednosti. Slično kontrolnim okvirima, programski okviri sadrže metodologiju (načine i uputstva) za procenu trenutnog i željenog bezbednosnog stanja organizacije, obezbeđujući kompletan set metrika kojima

se ova dva stanja mogu uporediti. Međutim, programski okviri sadrže i osnovne postupke za pravilnu procenu rizika, prioritizaciju zadataka i smernice za unapređenje komunikacije između tima za sajberbezbednost i menadžera/izvršnih rukovodilaca. Ukoliko je prvi faktor uspeha stručan i posvećen IT tim, adekvatna komunikacija kroz sve nivoe je svakako na visokom drugom mestu.

U poslednjoj grupi nalaze se okviri za upravljanje rizikom. Reč je o dokumentima u čijem je fokusu identifikacija, merenje i prioritizacija bezbednosnih rizika, odnosno definisanje procesa za procenu i upravljanje rizikom (tehnologije). Ovaj pristup upravljanju sajberbezbednosti teorijski je najispravniji, ali u praksi teško primenjiv u sistemima gde određeni IT procesi već funkcionišu uspešno. Razlozi tome su višestruki, a najvažniji su apstraktan jezik / terminologija i velika „udaljenost" od tehnologije i konkretnih, praktičnih primena.

Očekivanja, implementacija, cena

Iako u praksi verovatno nećete naići na situaciju da se prvo bira grupa (tip) okvira, pa tek onda neki konkretan okvir koji toj grupi pripada, korisno je znati osnovne prednosti svakog tipa zato što su očekivanja, vreme implementacije, kompleksnost i ukupna cena jedne ovakve „avanture" različiti. I ovde je pravi trenutak da ukažemo na drugu najčešću grešku koja se u praksi sreće – izbor zvučnog imena, odnosno okvira za koji ste dobili preporuke ili pročitali da „rešava sve probleme". Iako će u određenim situacijama preporuka biti od koristi, vratite se na ciljeve svoje organizacije koji ne moraju biti isti pa čak ni slični sa ciljevima i misijom organizacije gde je preporučeni okvir implementiran. I dobro promislite da li je to „odelo" skrojeno baš prema vašim merama.

Jedan od najpopularnijih okvira za upravljanje sajberbezbednošću je međunarodni standard ISO 27001, zvani još i ISO 27k. Organizacije koje imaju validan sertifikat u značajnoj su prednosti na tržištu jer su dokazale da sajberbezbednosti pristupaju sistematizovano, kao i da su sposobne da upravljaju bezbednosnim rizicima, što donosi veće poverenje klijenata, partnera i regulatora

Jedan od najpopularnijih okvira za upravljanje sajberbezbednošću, globalno ali i na našim prostorima, predstavlja međunarodni standard za upravljanje informacionom sigurnošću ISO 27001. Kroz ISO 27k (kako se drugačije obeležava), definišu se zahtevi za uspostavljanje, implementaciju, održavanje i stalno unapređenje sistema upravljanja informacionom sigurnošću (ISMS). ISO 27k standard spada u programske okvire i primenjiv je na organizacije svih veličina i tipova. Postoji više praktičnih razloga zašto je ISO 27k prvi (i često najbolji) izbor za uređenje informacione bezbednosti, a među najznačajnijima su visoka usklađenost sa zakonskim zahtevima i propisima koji se odnose na zaštitu informacija, smanjenje potencijalnih troškova prilikom pojave bezbednosnog incidenta i široka rasprostra-

Svaki od okvira, osim što znatno unapređuje sajberbezbednost, unapređuje i poslovne procese koji su osnov bezbednosnih programa, na prvom mestu procese brzog i kontrolisanog prilagođavanja novim izazovima

njenost, odnosno dostupnost znanju i iskustvu. Verovatno najvažniji je mogućnost sertifikacije, odnosno nezavisne provere usklađenosti ISO 27k kontrola u praksi. Organizacije koje imaju validan sertifikat, u značajnoj su prednosti na tržištu jer su dokazale da sajberbezbednosti pristupaju sistematizovano, kao i da su sposobne da upravljaju bezbednosnim rizicima, što posledično donosi veće poverenje klijenata, partnera i nadležnih regulatora. Ipak, fer je upozoriti da je implementacija ISO 27k u praksi veoma zahtevna, pa ne predstavlja najbolji izbor za manje kompanije ili sisteme s niskim nivoom zrelosti informacione bezbednosti. Barem ne kao prvi izbor.

CSF i CSC SCS okviri

Naredni okvir naziva NIST CSF *(National Institute of Standards and Technology Cybersecurity Framework),* razvijen je kao direktna potreba da se uredi metodologija zaštite IT sistema u okviru kritične infrastrukture SAD. Takođe je reč o programskom okviru koji neophodne kontrole grupiše u šest funkcija visokog nivoa (Identifikuj, Zaštiti, Otkrij, Odgovori na napad, Oporavi sisteme i servise i Upravljaj svim prethodnim funkcijama), čiji cilj je da složeni svet bezbednosti razloži na jednostavne kategorije koje modeliraju životni ciklus svih bezbednosnih aktivnosti. Njegov glavni adut je jednostavnost terminologije, koja bez „suvoparnih" tehničkih izraza, predstavlja jasno razumljive smernice koje treba sprovesti kako zaposlenima u IT sektorima, tako i visokom rukovodstvu.

CSF je dizajniran tako da bude fleksibilan i prilagodljiv različitim organizacijama, bez obzira na veličinu, industriju ili specifične potrebe i za razliku od ISO 27k okvira, ne postoji sertifikacija. Upravo ovaj „detalj" koji se ne čini kao prednost, omogućio je univerzalnu prihvaćenost širom sveta jer se CSF može koristiti ili nezavisno ili u kombinaciji s drugim standardima kako bi se poboljšala sajberbezbednost u kritičnim tačkama koje drugi okviri možda ne pokrivaju dovoljno detaljno.

Malo je verovatno da se organizacija koja se nije odredila ni prema jednom okviru odluči za bilo koji drugi osim ISO 27k ili NIST CSF okvira, ali u retkim situacijama, odličnu alternativu predstavlja i *Center for Internet Security Critical Security Controls* (CIS SCS okvir). Reč je o standardizovanim smernicama i alatima koji pomažu organizacijama da uspostave konzistentne i efikasne strategije odgovora na bezbednosne pretnje i da usklade svoje već implementirane prakse s drugim standardima i regulativama. Za razliku od prethodna dva standarda, koji imaju više od 100 specifičnih kontrola, CIS sadrži samo 20, ali nisu detaljne u zahtevima, ostavljajući mogućnost fleksibilnije implementacije. U svakom smislu, CIS propisuje efikasne mere organizacijama koje ne podležu obaveznim bezbednosnim protokolima i proverama, ali ipak žele da poboljšaju sajberbezbednost svojih okruženja. Druga značajna razlika (i prednost) jeste to što okvir počinje osnovama, prelazi na temeljne kontrole, a završava organizacionim unapređenjima, odnosno pomaže da prateći princip „odozdo naviše" na kontrolisan način dovede organizaciju do unapređenja sajberbezbednosti.

Mapiranje

Šta ako pogrešite u izboru okvira, shvativši negde na sredini implementacije da je drugi okvir bio bolji izbor? Ili se okolnosti prosto promene, s obzirom na brzinu promena kojima svedočimo u modernom poslovanju? Srećom, svi navedeni okviri, ali i većina drugih, kao obavezan deo sadrže i tzv. mapiranje kontrola na kontrole drugih okvira, praveći jasne relacije između istih ili sličnih oblasti i konkretnih zahteva. Iskustva iz prakse pokazuju da je ovakva tranzicija stresan korak, ali da nije komplikovan; poklapanje između različitih okvira je najčešće veće od 80 odsto. To konkretno znači da će dodatni napor biti maksimalnih 20 odsto kontrola (a često i manje), i to u slučajevima kada je realizacija projekta implementacije jednog od okvira već završena.

Ako je jedan ovakav projekat uspešno realizovan, velike su šanse da organizacija sa znatno manje napora samo „dopuni" odgovore na kontrole koje su različite. Jer, svaki od okvira, osim što znatno unapređuje sajberbezbednost, ne manje efikasno unapređuje i poslovne procese koji su osnov bezbednosnih programa, na prvom mestu procese brzog i kontrolisanog prilagođavanja novim izazovima. Sličan obim posla očekuje se i prelaskom na novu verziju okvira, ali sav taj „napor" vredniji je od napora koji vas čeka ukoliko dođe do bezbednosnog incidenta u nedovoljno uređenom sistemu.

Probajte prvo NIST CSF. Ako vam se posle prvih nekoliko koraka čini da sve deluje komplikovano, probajte CIS, u protivnom hrabro razmišljajte o ISO 27k implementaciji i sertifikaciji

Najvažniji korak u projektu implementacije bezbednosnog okvira predstavlja odluka da načinite prvi korak. Pravilno uspostavljen, svaki od navedenih standarda znatno će unaprediti ne samo bezbednosne kontrole, smanjujući i negativan uticaj i verovatnoću mogućih napada, nego i razumevanje poslovne vrednosti aktivnosti koje su timovi preduzeli. A prvi rezultati biće vidljivi nakon prvog uspešno otkrivenog, a neuspešno realizovanog napada; svedočenja su mnogih da je taj trenutak predstavljao prelomni momenat u daljem napretku ukupne zrelosti informacionih sistema uopšte. Ukoliko vam je ipak važna naša konkretna preporuka, evo je – probajte prvo NIST CSF. Ako vam se posle prvih nekoliko koraka čini da sve deluje komplikovano, probajte CIS, u protivnom, razmišljajte hrabro o ISO 27k implementaciji i sertifikaciji.

KORISNI LINKOVI

ISO 27k: https://www.iso.org/isoiec-27001-information-security.html

NIST CSF: https://www.nist.gov/cybersecurity

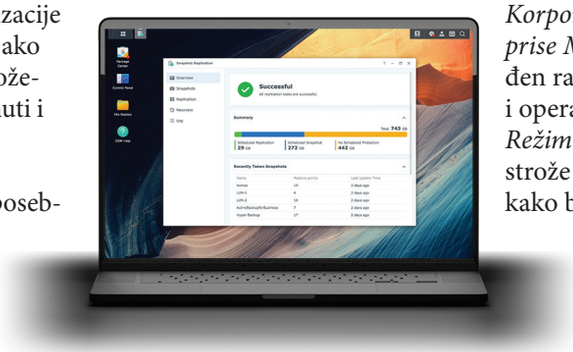
CIS CSC: https://www.cisecurity.org/controls

Poboljšanje integriteta podataka Synology Immutable Snapshots i WORM tehnologijama

U današnjem digitalnom okruženju obezbeđivanje integriteta i sigurnosti podataka od suštinskog je značaja. Najnovija unapređenja u DiskStation Manager-u (DSM) 7.2 kompanije Synology donose robusna rešenja sa Immutable Snapshots *i* Write Once, Read Many (WORM) tehnologijom, osmišljenim da zaštite podatke od neovlašćenih izmena i sajberpretnji

Neizmenjive kopije podataka

Immutable Snapshots, izuzetna funkcionalnost u DSM 7.2, pružaju siguran način za čuvanje kopija podataka koje se ne mogu menjati ili brisati. Ova funkcionalnost je ključna za odbranu od *ransomware* napada i slučajnog gubitka podataka. Kreiranjem neizmenjivih kopija podataka u određenim intervalima, organizacije mogu osigurati da čak i ako su primarni podaci ugroženi, snimci ostaju netaknuti i dostupni za oporavak.



Ova funkcionalnost je posebno korisna za okruženja gde je integritet podataka ključan, kao što su finansijske institucije, zdravstvene ustanove i pravne firme. Neizmenjivi snimci pomažu u ispunjavanju regulatornih zahteva i pružaju sigurnost da su osetljivi podaci zaštićeni od neovlašćenih izmena.

Write Once, Read Many (WORM): sprovođenje politika zadržavanja podataka

WORM tehnologija u *Synology*-jevom DSM-u 7.2 omogućava kreiranje *WriteOnce* deljenih foldera, koji su dizajnirani da spreče bilo kakvu izmenu ili brisanje podataka nakon što su napisani. Ovo je posebno korisno za organizacije koje moraju da se pridržavaju strogih politika zadržavanja podataka. WORM osigurava da podaci ostaju nepromenjeni tokom definisanog perioda ili zauvek, u zavisnosti od potreba organizacije.

Synology nudi različite režime za WORM foldere, uključujući *Režim usklađenosti* (*Compliance Mode*) i *Korporativni režim* (*Enterprise Mode*), svaki prilagođen različitim regulatornim i operativnim potrebama. *Režim usklađenosti* sprovodi strože politike zadržavanja kako bi ispunio pravne i regulatorne standarde, dok *Korporativni režim* nudi fleksibilnost za interne potrebe zaštite podataka.

Poboljšana sigurnost i performanse

Pored neizmenjivih snimaka i WORM-a, DSM 7.2 uvodi funkcije kao što su enkripcija celokupnog volumena i adaptivna multifaktorska autentifikacija (AMFA) za poboljšanje sigurnosti. Enkripcija celokupnog volumena štiti podatke u mirovanju enkripcijom celokupnih skladišnih volumena, čime se štiti od fizičke krađe i neovlašćenog pristupa.

Integracija AMFA daje dodatni nivo sigurnosti zahtevajući više oblika verifikacije pre nego što se odobri pristup sistemu, posebno s nepoverljivih izvora. Ovo smanjuje rizik od neovlašćenog pristupa čak i ako su kompromitovane pristupne informacije.

Pored toga, DSM 7.2 uključuje poboljšanja performansi, kao što su deduplikacija na nivou blokova i poboljšane brzine *backup*-a *Hyper Backup*-om, obezbeđujući da zaštita podataka ne ugrožava performanse sistema.

Na kraju...

Synology-jev DSM 7.2 s neizmenjivim snimcima i WORM tehnologijom nudi sveobuhvatno rešenje za organizacije koje žele da poboljšaju integritet i sigurnost svojih podataka. Integracijom ovih naprednih funkcija *Synology* osigurava da podaci ostaju zaštićeni, usklađeni i lako obnovljivi, pozicionirajući se kao lider u rešenjima za upravljanje i zaštitu podataka.

Za više detalja o ovim funkcijama i kako mogu koristiti vašoj organizaciji, posetite zvanični sajt *Synology* i stranice s korisnim informacijama:

www.synology.com/DSM72
blog.synology.com
www.synology.com/company/news
www.synology.com/en-eu

Zaštita kritične IT infrastrukture - OPSWAT

OPSWAT je kompanija koja nudi rešenja za IT i OT sektor u domenu sajberbezbednosti. Glavni cilj OPSWAT-a je postići što veći stepen automatizacije u detekciji potencijalnih pretnji kako bi se napadi mogli primetiti i sprečiti pre nego što započnu

Pavle Petrović, inženjer za sajber bezbednost, Co.Next

MetaDefender Core namenjen je za prevenciju pretnji koje dolaze, pre svega, preko malicioznih fajlova i *zero-day eksploit*-a. Postavlja se u već postojeću infrastrukturu i pruža zaštitu od najčešćih vrsta napada: malver, eksfiltracija podataka, korišćenje ranjivosti u određenim tipovima fajlova (*file-based vulnerabilities*). Može se koristiti za zaštitu *Web* portala i fajl servera od *upload*-a malicioznih fajlova, ali i za manuelno skeniranje fajlova.

MD *Core* se sastoji od nekoliko modula koji, svaki za sebe, pružaju veliki broj mogućnosti po pitanju zaštite infrastrukture jedne kompanije:

MetaScan/Multiscanning: simultano skeniranje i analiza fajlova izborom skupa antivirusnih *engine*-a više od 30 AV proizvođača.

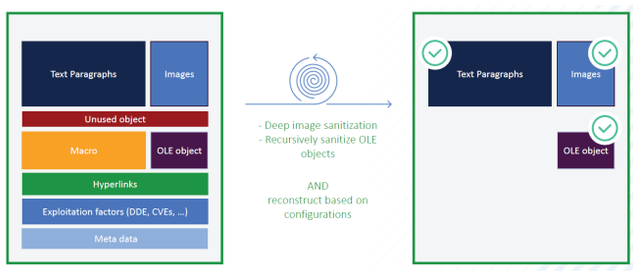
Deep CDR (Content Disarm and Reconstruction): pretpostavljajući da svaki fajl koji prolazi kroz mrežu, stiže u *mail*-u, preuzima ili šalje, sadrži potencijalnu pretnju, kao što je malver ili ranjivost koja se može iskoristiti pre nego što bude otkrivena, CDR tehnologija analizira i uklanja iz fajlova maliciozne linkove i ostali potencijalno štetni aktivni sadržaj. Fajlovi se zatim rekonstruišu i isporučuju korisniku uz zadržavanje metapodataka i ostalih karakteristika, tako da mogu da se bezbedno koriste bez gubitka upotrebljivosti. Originalni fajlovi stavljaju se u karantin radi pravljenja rezervnih kopija i daljeg pregleda. Sistem pruža detaljne informacije o neutralisanim i izmenjenim objektima za svaki fajl, omogućavajući vam da imate realni uvid, donosite prave odluke i konfigurišete tehnologiju tako da najbolje odgovara vašoj situaciji i strategiji.

CDR tehnologija analizira i uklanja iz fajlova maliciozne linkove i ostali potencijalno štetni aktivni sadržaj. Fajlovi se zatim rekonstruišu i isporučuju korisniku uz zadržavanje metapodataka i ostalih karakteristika, tako da mogu da se bezbedno koriste bez gubitka upotrebljivosti

Proactive DLP (Data Loss Prevention): fajlovi koji se šalju mogu da sadrže osetljive i bitne podatke. Određeni tipovi fajlova se proveravaju i u slučaju da se otkriju osetljivi podaci, mogu da se povuku pre njihovog slanja.

Sandbox: pruža analizu fajlova koji potencijalno sadrže malver, u posebnom, izolovanom okruženju. *Sandbox* se podiže *on-premise* (na lokaciji korisnika) brzo i jednostavno, a jedan server može da obradi više od 25.000 fajlova dnevno. Znatno je brži od klasičnih *sandbox* rešenja. Nudi statičku i dinamičku analizu pretnji uz korišćenje vlastite baze znanja i mašinsko učenje.

Threat Intelligence: ovaj modul je, u stvari, poseban *engine* koji sakuplja informacije od drugih korisnika OPSWAT tehnologija i time omogućava *real-time* uvid u potencijalne pretnje.



File-based Vulnerability: detekcija poznatih ranjivosti u fajlovima za veliki broj aplikacija.

Zaštita elektronske pošte

MetaDefender Mail Security je rešenje za zaštitu *e-mail* servera. Može se ugraditi u mreže s već postojećim mejl serverima, a postoji i mogućnost integracije u sisteme koji koriste *cloud mail* provajdere. Podržan je i *Microsoft* 365.

MD Mail Security koristi neke delove (module) prethodno navedene platforme MD *Core*, i sprečava česte metode napada preko mejla, kao što su *phishing*, *spam* i malver koji je sadržan u priloženim fajlovima. MD *Mail Security* licencira se po broju instanci za pristup (*email gateway*), a za *cloud* rešenje licencira se po broju korisnika.

MetaDefender Kiosk analizira prenosive uređaje i medijume: USB memoriju, CD/DVD romove, SD i *microSD* kartice, i druge. Kiosk se postavlja na periferiji mreže, i time se maliciozni fajlovi detektuju pre nego što uđu u mrežu same kompanije i nanesu štetu. Kiosk je pogodan za korišćenje u proizvodnim pogonima, energetskim postrojenjima, u suštini, na bilo kom mestu gde se svakodnevno koriste prenosivi *media* uređaji.

Za dodatne informacije, prikaz ili testiranje u vašem okruženju, obratite se preduzeću *Co.Next* iz Beograda, distributeru OPSWAT-a.

co-next.eu

Comtrade Cloud: prednost u poslovanju savremenih kompanija

Cloud Computing donosi razne benefite kompanijama. Jedan od njih je omogućavanje IT stručnjacima da svoje vreme usmere na druge poslove, a ne na održavanje IT infrastrukture

Đorđe Nedeljković, Senior Presales System Engineer

Prethodne godine pokazale su nam da postoji oskudica IT profesionalaca na tržištu - pre svega zbog naše sve veće i učestalije saradnje i komunikacije s krajnjim korisnicima. Kompanije i dalje imaju potrebu za održavanjem, unapređivanjem i kreiranjem trenutnih i novih tehnologija zarad podržavanja poslovnih procesa i sistema, a da bi imale uopšte mogućnost za to, potrebno je da poseduju dobro obučeno i efikasno IT osoblje koje je teško naći, pa se javlja problem. Jedno od rešenja je *cloud*.

Cloud computing predstavlja jedinstveno rešenje problema i donosi razne prednosti kompanijama. Jedan od njih je omogućavanje IT stručnjacima da svoje vreme usmere na druge poslove, a ne na održavanje IT infrastrukture.

Pored manjka IT osoblja, dodatni izazov s kojima se organizacije suočavaju jeste i nabavljanje novih sistema za određeni period. Stalno nadgledanje i obnavljanje infrastrukturnih sistema dovodi do lošije procene neophodnih resursa za poslovanje i bojazni da neki od njih zafali. Zahvaljujući mogućnosti plaćanja samo onih resursa koji se koriste, *cloud* rešenja pružaju sigurnost u postojanje uvek dovoljnih kapaciteta i neograničenog širenja u slučaju potrebe. Takođe, ako je potrebno povećanje ili smanjenje računarskih resursa, odnosno skaliranje, oni se izvršavaju gotovo trenutno i bez potrebe za nabavkom dodatnih hardverskih resursa i značajnih troškova. Ukoliko kompanije ne poseduju sopstvene *data* centre, izgradnja ili iznajmljivanje donosi dodatne troškove. *Cloud* rešenja u svojoj osnovi obezbeđuju nekoliko *data* centara na geografski udaljenim lokacijama, što automatski pruža prednost korisnicima, jer ne moraju da samostalno vode brigu o svojim *data* centrima i opremi u njima.

Zahvaljujući lokalnim data centrima, Comtrade Cloud ima prediktivan trošak zakupa resursa bez promene mesečnog troška u slučaju nepromenjenih zakupljenih resursa. Platforma je kreirana shodno korisničkim potrebama i funkcioniše u saradnji i partnerstvu sa svim vodećim vendorima

Comtrade Cloud

Kada govorimo o *Comtrade Cloud*-u, prepoznajemo javna i privatna *cloud* rešenja. Javno predstavlja okruženje u kome iste resurse deli veći broj kompanija, naravno, u potpuno zaštićenom i definisanom okruženju, a privatno se odnosi na okruženje u kome jedna kompanija koristi posvećene resurse, bez deljenja s drugim korisnicima.

Comtrade Cloud je lokalni *cloud* provajder. U kontekstu prethodno navedenih prednosti *cloud*-a u odnosu na IT infrastrukturu na samoj lokaciji, on se izdvaja po sledećim odlikama:

- Robusna lokalna infrastruktura razdvojena je u tri geografski udaljena *Tier* 3/4 *data* centra na teritoriji Srbije i EU.
- Više od dve decenije tehnološki građene ekspertize, počev od dizajniranja arhitekture rešenja sve do implementacije kritičnih okruženja, pokazujući duboko razumevanje i tehničku širinu.
- GDPR usklađenost zahvaljujući prisustvu na teritoriji EU.
- Fleksibilne implementacije shodno potrebi za različitim tehnologijama, poput *VMware*, *Open Source* i *Open Stack* sistema.
- Korisnički orijentisana podrška različitih nivoa: *Basic*, *Standard*, *Premium* i *Managed*.

Kao lokalni *cloud* provajder, **Comtrade Cloud** pruža i dosta prednosti u odnosu na javne *cloud* provajdere. On osigurava suverenitet podataka i podržavanje lokalnih zakona, kao i čuvanje podataka u okvirima teritorije na kojoj kompanije posluju. Pored toga, obezbeđuje veću brzinu i manje kašnjenje u komunikaciji s poslovnim sistemima. Zahvaljujući lokalnim *data* centrima, *Comtrade Cloud* ima prediktivan trošak zakupa resursa bez promene mesečnog troška u slučaju nepromenjenih zakupljenih resursa. Platforma je kreirana shodno korisničkim potrebama i funkcioniše u saradnji i partnerstvu sa svim vodećim vendorima, te pruža podršku za prioritetno rešavanje problema, ako se pojave.

Potrebe trenutnog tržišta sve više ukazuju da će postojati integracija lokalnih i javnih *cloud* provajdera, a ukoliko vas zanima koje *cloud* rešenje je idealno za vašu kompaniju, posetite naš sajt **www.comtradeintegration.com** gde možete pronaći više informacija i kontaktirati sa stručnjacima koji mogu da vam pomognu u proceni.

Comtrade System Integration
www.comtradeintegration.com

Zaštita tajnih i poverljivih informacija nikada nije bila važnija za organizacije

Da bi opstale, kompanije ne mogu da izbegnu digitalnu transformaciju. Uz dugi niz prednosti koje donosi - povećanu efikasnost, poboljšano korisničko iskustvo, veću fleksibilnost, održivi rast i pristup globalnom tržištu - digitalna transformacija takođe može dovesti do većih bezbednosnih rizika

Lagana nepažnja ili greška u upravljanju tokenima, sertifikatima ili API ključevima dovoljna je da napadač neovlašćeno „uđe“ u interne servise kompanije. Rezultat je sve veće „curenje“ tajnih podataka.

Čak i najmanja greška je dovoljna da tajni podaci - ključevi za šifrovanje, API tokeni, akreditivi i sertifikati - dođu u pogrešne ruke, što otvara put ka internim resursima. Jednom otkrivena, tajna može postati ozbiljna pretnja kompanijama.

M2M (*machine to machine*) autorizacija, odnosno komunikacija i razmena podataka između različitih uređaja bez ljudske intervencije, svakodnevno dovodi do bezbednosnih izazova. Upravo akreditivi koji su ukradeni tokom ovog procesa daju napadačima pristup internim servisima. Prema istraživanju, više od 60 odsto svih neovlašćenih ulaza u resurse kompanije uključuje ukradene pristupne podatke. Jasno je da zaštita takvih podataka, kao i drugih koji spadaju u kategoriju tajni, postaje bezbednosni prioritet.

Da bi funkcionisale nesmetano, kompanije moraju da obezbede nesmetanu komunikaciju između različitih aplikacija, mikroservisa i radnih okruženja *(workflow)*. Protokoli koji stoje iza takve komunikacije spadaju u kategoriju tajni i moraju biti zaštićeni po svaku cenu.

Disperzija poverljivih informacija je neizbežna. Naime, podaci svakodnevno putuju iz jednog okruženja u drugo - na primer, iz jednog oblaka u drugi. Tako danas nalazimo tajne podatke na nivou CI/CD cevovoda, u *slack* kanalima i na mnogim drugim mestima. Stoga je jasno da uprav-

ljanje tajnama treba da bude centralizovano.

Kako broj *DevOps* timova raste, raste i softverska kodna baza. Bez efikasne zaštite, njihovo funkcionisanje je ugroženo. Naime, bez pravilnog upravljanja tajnama, jedini način na koji softverski sistemi mogu da dobiju pristup jedan drugom jeste ručno deljenje tajni unutar timova i njihovo ugrađivanje u kod. Možemo pretpostaviti da će se u praksi ovo završiti upotrebom veoma slabih lozinki - i to za niz različitih sistema. Zaštita tajni je, naravno, zbog toga teža.

Upravljanje tajnama je od suštinskog značaja

Neki od najvažnijih razloga zašto je upravljanje tajnama od suštinskog značaja i treba da postane prioritet kompanija su:

• Količina podataka stalno raste
Neki analitičari predviđaju da će se *Global DataSphere* (IDC-jev sistem za kvantifikaciju i analizu količine podataka stvorenih, snimljenih i repliciranih u bilo kojoj godini širom sveta) udvostručiti do 2026. Ova informacija je posebno značajna ako znamo da tek nešto više od 50 odsto kompanija zna gde se njihovi podaci čuvaju.

• Broj propisa i zakona raste
Zaštita podataka je već dugi niz godina u fokusu zakonodavaca i regulatornih tela, pa shodno tome raste i broj propisa kojih kompanije moraju da se pridržavaju u svakodnevnom radu. Međutim, više od 40 procenata osetljivih podataka uskladištenih u oblaku ostaje nešifrovano.

• Upravljanje postaje sve složenije
Složenost je tradicionalno glavni izazov u zaštiti podataka. Dodatni problem predstavlja činjenica da je više od polovine podataka unutar preduzeća neklasifikovano.

• Broj napada se povećava
Povećava se broj neovlašćenih pristupa internim servisima i poverljivim informacijama kompanija. Samo nešto više od polovine kompanija ima potpunu kontrolu nad ključevima za šifrovanje i pristupom šifrovanim podacima u oblaku.

Kompletna zaštita uz Thales CipherTrust Secrets Management

Thales CipherTrust Secrets Management omogućava efikasno upravljanje, skladištenje i pristup tajnama. Rešenje obezbeđuje automatizovanu rotaciju tajni i poštovanje propisa.

Ključne funkcije *CipherTrust Secrets Management*-a uključuju:

- centralizovano upravljanje tajnama,
- bezbedno skladištenje sa šifrovanjem,
- kontrolu pristupa,
- automatsku rotaciju tajni i
- praćenje svih aktivnosti i generisanje izveštaja.

exclusive-networks.com/rs/

B&F BIZNIS & FINANSIJE

Pretplatite se na štampano i elektronsko izdanje magazina Biznis i Finansije za 2024.
U cenu pretplate na magazin uračunate su Specijalne godišnje edicije: Finansije TOP, Biznis TOP, MSP

Vreme je za nas

Više informacija
www.bif.rs
marketing@bif.rs
pretplata@bif.rs

Univerzalno isplativo rešenje za bekap i oporavak podataka

Čuvanje rezervnih kopija i disaster recovery rešenja danas je neizostavno u svakom ozbiljnom poslovnom okruženju. Međutim, mnogi proizvođači koji se bave razvojem ovih rešenja fokusirani su na velike firme. Manja i srednja preduzeća mogu da koriste ta rešenja, ali su troškovi često preveliki, pa se to ne može okarakterisati kao finansijski isplativa solucija

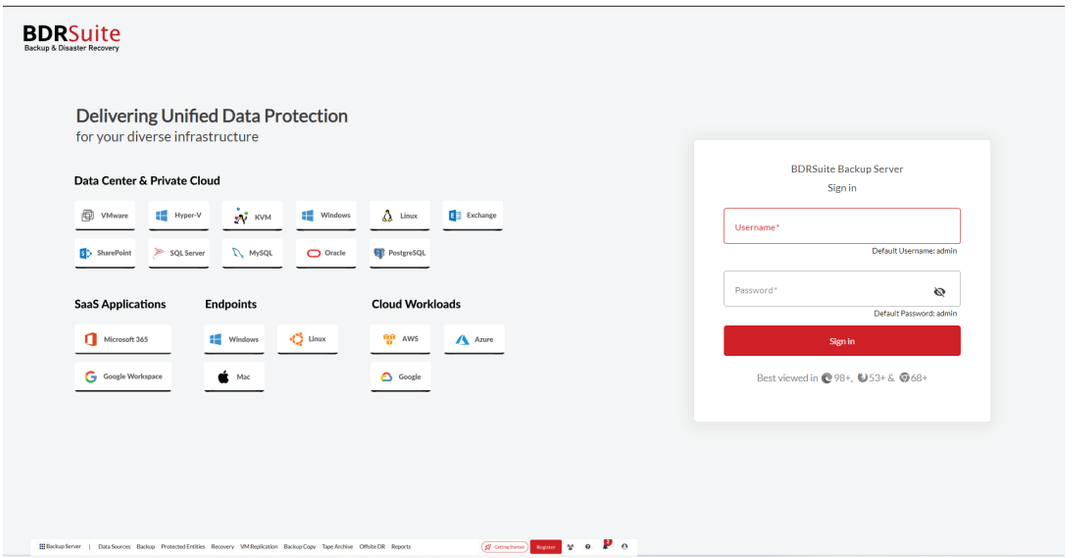
Branislav Bubanja

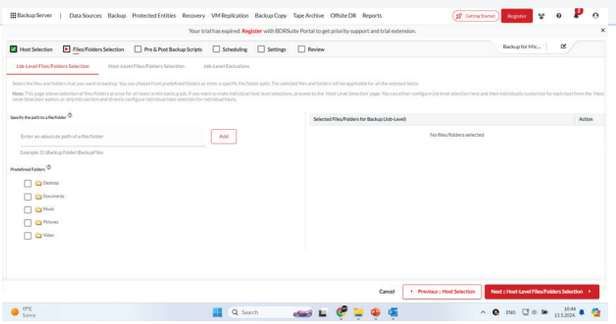
Tu svoje mesto pronalazi *Vembu BDRSuite*. Reč je o pouzdanom proizvodu atraktivne cene, namenjenom malim i srednjim preduzećima. Njegova glavna odlika je da je jednostavan za upotrebu, tako da u slučaju potrebe svaki korisnik može brzo da oporavi oštećene ili obrisane podatke.

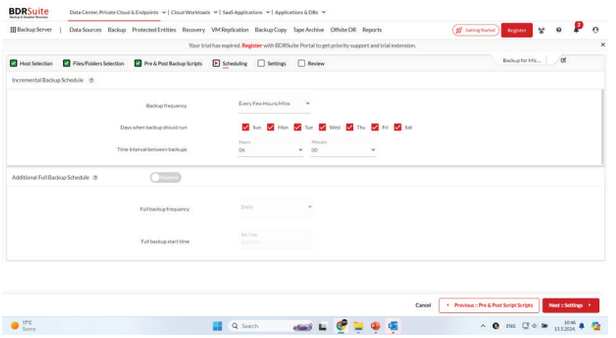
Fleksibilno rešenje

BDRSuite je sveobuhvatno rešenje za pravljenje rezervnih kopija i oporavak posle katastrofe, dizajniran za zaštitu najrazličitijih poslovnih okruženja. Napravljen je da zaštiti podatke na virtuelnim mašinama (*VMware*, *Hyper*-V, KVM, *oVirt*, *Proxmox*), serverima (*Windows*, *Linux*, NAS), računarima (*Windows*, *Linux*, *Mac*), *SaaS* aplikacijama (*Microsoft* 365, *Google Workspace*), *cloud* radnim okruženjima (AWS, *Azure*), kao i na aplikacijama i bazama podataka (*Microsoft Exchange Server*, SQL *Server*, *SharePoint*, *MySQL*, *PostgreSQL*). Fokus *BDRSuite*-a su kompanije do 50 zaposlenih, ali to ne znači da nije upotrebljiv i u većim poslovnim okruženjima. Pored njega, korisnicima je na raspolaganju i *cloud* rešenje zasnovano na istoj platformi - *BDRCloud*.

Iako je na našem tržištu ovo nov proizvod, u svetu je poznato i priznato rešenje. Kompanija *Vembu*, koja stoji iza njega, ima dugogodišnje iskustvo. Ona je na *Backup* & *Disaster Recovery* tržište ušla još 2002.







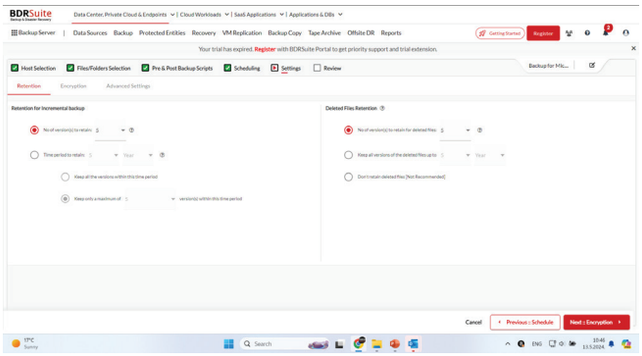
godine, a njihova rešenja koristi više od 60.000 kompanija širom sveta. *BDRSuite* je stekao odličnu reputaciju, jer je jednostavan i moćan alat koji podržava tzv. „3-2-1“ politiku pravljenja rezervnih kopija. Ta politika podrazumeva pravljenje **tri** kopije rezervnih podataka, koje se čuvaju na **dva** različita medija (kao što su diskovi, magnetne trake ili *cloud*), od kojih se **jedna** kopija čuva na nekoj udaljenoj lokaciji. Ovakav pristup znatno smanjuje rizik od gubitka podataka usled kvara hardvera, *ransomware* napada ili usled prirodnih katastrofa.

Centralizovana kontrola

BDRSuite obezbeđuje centralizovano upravljanje i monitoring bekapa u okruženju koje korisniku najviše

odgovara, na bilo kojoj platformi (virtuelnoj, fizičkoj, u *Docker*-u ili *cloud*-u). Kompletno nadgledanje sistema obavlja se preko *Web* zasnovane konzole. Glavne karakteristike ove platforme su da omogućava bekap najrazličitijih IT okruženja, fleksibilan i brz povratak podataka, kao i efikasnu zaštitu od *ransomware* napada.

Podržan je bekap virtuelnih mašina, diskova, fajlova i foldera i baza podataka, koji se obavlja u skoro realnom vremenu. Kako bi se osigurala konzistentnost bekapovanih podataka, uključena je automatska verifikacija. I proces oporavka je fleksibilan. Oporavak virtuelnih mašina je moguć za nekoliko minuta, podržan je oporavak na nivou fajlova, kao i oporavak podataka u *Microsoft Azure* okruženju, odnosno za *Microsoft Exchange*, SQL, *SharePoint*, *Active Directory*… Dodatnu sigurnost obezbeđuju detekcija anomalija, višestruki bekap, skeniranje fajlova u potrazi za *malware* komponentama pre samog čina bekapovanja… Sve to obezbeđuje potpunu zaštitu od



ransomware napada, kao i dodatni nivo sigurnosti rezervnih kopija.

Dodatne funkcije

Pored navedenih, veoma važne karakteristike *BDRSuite*-a jesu i moćne funkcije oporavka podataka koje uključuju replikaciju virtuelnih mašina, čuvanje podataka u udaljenim *data* centrima i *cloud* zasnovan *disaster recovery* sistem. Bekapovani fajlovi su enkriptovani i kompresovani, a da bi im se pristupilo, neophodna je dvofaktorska autentifikacija. Sve akcije koje se obavljaju, čuvaju se u log fajlovima i mogu da se pregledaju kroz odličan *reporting* sistem.

Ipak, najvažnija karakteristika *BDRSuite*-a jeste ta da održava kontinuitet poslovanja, jer je oporavak bekapovanih mašina veoma brz - *Vembu* tvrdi da će svaka mašina biti ponovo operativna za manje od 15 minuta od početka *recovery* procesa.

Za male i srednje kompanije su optimizacija i kontrola troškova od presudne važnosti. *Vembu* je svestan toga, pa *BDRSuite* licence mogu da se kupe na osnovu različitih kriterijuma - prema broju virtuelnih mašina, servera, CPU *socket*-a, broju korisnika… Takođe, na raspolaganju su i različite edicije platforme, pa kompanije mogu da nađu najbolji (finansijski najprihvatljiviji) modus koji će pokriti sve njihove potrebe. Ovakva fleksibilnost omogućava *BDRSuite* korisnicima da ostvare uštede do čak 70 procenata na cenu bekapa i oporavka podataka u odnosu na slična rešenja drugih kompanija.

Singi.rs

Iznajmite PC Press Studio za snimanje podkasta!

Do studija lako! • marketing@pcpress.rs • 011/276-55-33