Data centri 2022.

Specijalni dodatak časopisa PC Press #299

Data centri

Paralelno s razvojem i porastom značaja podataka koje kreiramo, razmenjujemo i skladištimo u digitalnom formatu, rastao je i značaj ključne IT infrastrukture namenjene upravljanju tim podacima. Data centar je osnovna komponenta te infrastrukture, a njegovo projektovanje i održavanje predstavlja veoma ozbiljan izazov

Dušan Katilović

Energija i bezbednost postulati data centra

Industrija informacionih tehnologija ima višedecenijsko iskustvo u vezi s *data* centrima – specijalizovanim prostorima ili objektima u kojima se drži informatička i komunikaciona oprema s pripadajućim sistemima napajanja energijom. Projektovanje, izgradnja i održavanje *data* centara dotiču se mnogih drugih polja ljudske delatnosti: prostornog planiranja (s geodezijom, meteorologijom i seizmologijom), zaštite od požara, perimetarnog i fizičko-tehničkog obezbeđenja, HVAC (grejanja, ventilacije i tretiranja vazduha), arhitekture, energetike, inženjerstva, ekologije i drugih.

Kako je *data* centar garant i osnova neprekidnosti poslovnih procesa, cilj njegovog vlasnika/operatora je da obezbedi apsolutnu pouzdanost u vidu 24/7/365 dostupnosti resursa koji se u njemu koriste. S obzirom na prirodu i zahtevnost prvih korisnika velikih *data* centara (vojska, naučno-istraživački centri, velike korporacije), mnoga tehnička rešenja u njima se već dugo koriste, ali su prilagođena savremenim tehnološkim dostignućima.

Katalizator buma koji su doživeli bio je dvostruk – eksponencijalni porast količine podataka u opticaju, kao i intenzivan proces izmeštanja tih podataka s lokalnih računara na *cloud*. Svaki *data* centar se oslanja na „svega“ dva osnovna postulata – energetsku efikasnost i bezbednost.

Imperativ energetske efikasnosti

Energetska efikasnost *data* centara je pitanje koje ih prati otkako postoje. Prvi *mainframe* sistemi bili su izuzetno veliki i neefikasni potrošači električne energije. Iako je prevaljen dug put u pogledu umanjenja potrošnje struje, sve je više servera i druge opreme koja se hostuje u *data* centru i to zahteva ogromne resurse. U situaciji kada ulazimo u duži period energetske oskudice i skupoće, ovo pitanje dodatno dobija na značaju.

Osim same količine raspoložive energije, za *data* centar je bitno obezbediti i neprekidnost i stabilnost u napajanju, tako da se neposredno pored njih po pravilu gradi i posebna trafo-stanica – energetski čvor.

Energetska efikasnost je preduslov finansijske održivosti *data* centra i ona se povećava ili linearnim (serijskim) unapređenjem centra kroz *upgrade* opreme ili njegovom konsolidacijom. Osnovni cilj konsolidacije je postizanje optimuma u radu centra, tj. dostizanje situacije da su njegovi kapaciteti dovoljno uposleni, ali ne i preopterećeni.

Iako koncepcijski jednostavan, ovaj cilj se nikada u stvarnosti ne može u potpunosti dostići, ali mu se efikasan centar može veoma približiti putem implementacije dinamičke infrastrukture koja predstavlja svojstvo hardvera i softvera unutar centra da se inteligentno prilagođava fluktuacijama u

intenzitetu eksploatacije resursa od strane korisnika.

Virtuelizacija i automatizacija – katalizatori napretka

Virtuelizacija predstavlja princip čijom primenom se *data* centar osposobljava da podržava potrebe klijenata za *cloud* infrastrukturom. *Cloud* infrastruktura izdvojena za određenog korisnika logički je zaokružen, segmentiran deo hardverskih kapaciteta centra koji se sastoji od virtuelnih servera, skladišta podataka i drugih komponenti neophodnih za funkcionisanje hostovanog IT sistema klijenta.

Sve učestalija virtuelizacija IT resursa jedan je od glavnih ekonomskih pokretača razvoja industrije *data* centara. Serveri i diskovi koji se nalaze u *cloud*-u kompanija unutar *data* centra smanjuju kapitalna ulaganja, umanjuju i ustaljuju operativne troškove (često u troškovno predvidivoj formi pretplate) i *outsource*-uju bezbednosna pitanja na viši nivo ekspertize.

Automatizacija *data* centara nije samo direktno pitanje optimizacije troškova, već ona doprinosi efikasnosti, a predstavlja i jedan od odgovora na sve izraženije pitanje globalnog manjka kvalifikovanih stručnjaka (IT inženjera). Aktivacija, migriranje, konfigurisanje, instalacija zakrpa i druge krucijalne radnje mogu se u *data* centru današnjice obavljati bez direktnog prisustva osobe zadužene za tehničku podršku. Ovaj koncept se često naziva „*data* centar u mraku“ jer u njemu, po pravilu, ne boravi niko, te osvetljenje nije potrebno.

Zeleni data centri

Iako se u proteklih 10-12 godina broj korisnika Interneta udvostručio a mrežni saobraćaj uvećao za 15 puta, globalna potrošnja tradicionalnih *data* centara je za to vreme beležila blagi trend opadanja. Prema podacima *Digital Realty* trasta, u svetu se na *data* centre godišnje potroši oko 90 milijardi kWh električne energije, što predstavlja oko 3% svetske potrošnje ili ekvivalent oko 35 termoelektrana većeg kapaciteta.

Pošto pitanje kontrole utroška energije odavno nije samo ekološko ili ekonomsko, već i političko pitanje od prvorazrednog značaja. Primetan je dugotrajan pritisak javnosti i vlasti na industriju *data* centara u smeru ka dostizanju cilja ugljeničke neutralnosti. Sami operatori su po prirodi stvari veoma zainteresovani za „zelene ciljeve“, naročito ako se uzme u obzir da je energija pojedinačno ubedljivo najveća stavka koja čini do 10% TCO (ukupnih troškova posedovanja), a „hod niz dlaku zelene agende“ donosi ne samo pozitivan PR, već i pristup izdašnim javnim investicionim fondovima.

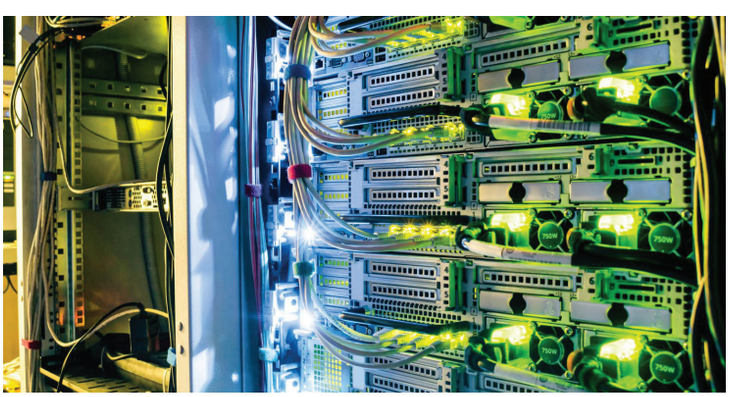
Vodeći zapadnoevropski igrači u ovoj industriji sklopili su Pakt o klimatski neutralnom *data* centru koji sledi ambiciozne ciljeve Evropske unije o dostizanju potpune ugljeničke neutralnosti do 2050, dok s drugih meridijana stižu neke slične vesti, ali ponegde i upadljiv izostanak obećanja o „zelenoj tranziciji“.

Bezbednosni protokoli

Bezbednost *data* centra čine protokoli, mere predostrožnosti i praktične akcije usmerene ka sprečavanju neovlašćenog pristupa i manipulacije resursima. *Denial of Service* napadi, krađa, neovlašćena izmena ili uništavanje poverljivih podataka su standardne digitalne sigurnosne pretnje po *data* centar koje mogu da naruše njegov integritet i reputaciju. Štete po korisnike mogu biti pogubne u scenariju kada su bitni podaci kompanije s njenih lokalnih servera izmešteni i uskladišteni na *cloud* unutar centra.

Pored čitavog niza bezbednosnih politika i protokola, sofisticirane IT opreme i obučenog kadra, *data* centru potencijalne pretnje dolaze ne samo iz digitalnog već i iz realnog sveta. Tako vodeći *data* centri poseduju kompleksne CCTV sisteme sa zadržavanjem snimaka do 90 dana, proverenu *(vetted) outsource*-ovanu ili internu službu fizičko-tehničkog obezbeđenja, operativno-komandni centar (NOC) osposobljen za brza dejstva, protokole ulaska, izlaska i zadržavanja u objektu s detektorima pristupa i kretanja i mnogo drugih procedura.

Najzad, ponekad se sve mere mogu ispostaviti kao nedovoljne, pa i spram ćudi prirode. Veliki centri se lociraju na mestima gde su minimalne šanse za nastupanje prirodne katastrofe i više sile, kao što su poplave, zemljotresi, vulkani, klizišta, cunamiji, a u slučaju akcidenta i proboja sigurnosti, aktiviraju se prethodno definisani mehanizmi oporavka od katastrofe *(disaster recovery)*, u šta može da spada i aktivacija sekundarnog postrojenja koje je fizički udaljeno od primarnog više desetina ili stotina kilometara.



Procesi stalne **optimizacije data centra**

Ključni kontinuirani transformacioni procesi od značaja za rad savremenog *data* centra su:

- Redovno obnavljanje opreme *(upgrade)*
- Konsolidacija (standardizacija)
- Virtuelizacija
- Automatizacija

Zaštita podataka sa IBM storidž sistemima

U okviru svog storidž portfolija, IBM je početkom 2022. predstavio, a Comtrade Distribution obogatio svoju IBM ponudu hardverskih rešenja sa dva nova modela iz FlashSystem familije – FlashSystem 7300 (FS7300) i FlashSystem 9500 (FS9500)

Miodrag Nikolić i Aleksandar Gagović, Comtrade Distribution

Slika 1. – IBM FS7300

Novi storidž sistemi poseduju bogat set funkcija koje su prilagođene za kritična opterećenja i aplikacije. Osnovne karakteristike ovih storidž uređaja su: *end-to-end* NVMe protokol, IBM *FlashCore* tehnologija i ultraniska latencija kroz *Storage Class Memory* (SCM) module.

Nove mogućnosti

Pored klasičnih funkcionalnosti koje IBM storidž sistemi pružaju, postoji i nekoliko karakteristika koje ove uređaje izdvajaju kao najbolje u klasi. Predstavljamo njihove mogućnosti

Redundantnost visokih performansi: NVMe drajvovi visoke dostupnosti u 2U šasiji (FS7300) i 4U šasiji (FS9500) za skladištenje s mrežnom replikacijom na tri lokacije kako bi se postigla dostupnost u svakom trenutku – *No Single Point of Failure* (NSPOF).

Skalabilnost za okruženja različitih veličina: pametnim kontejnerskim rešenjem lako se upravlja, omogućavajući kompanijama da prevaziđu izazove skladištenja.

Rešenje visoke vrednosti koje je pristupačno: funkcionalnosti fleš-memorije visoke gustine u pristupačnom paketu uključuju kompresiju, novu QLC tehnologiju zasnovanu na fleš-memoriji i prediktivnu analitiku zasnovanu na veštačkoj inteligenciji.

Agilna integracija: migracija podataka s potpuno integrisanim upravljanjem sistemom i funkcionalnostima visoke vrednosti, kao što su AES enkripcija i *inline* hardverska kompresija.

Multicloud: mogućnost rada u *multicloud* okruženju.

Čvrsta otpornost: IBM softver *Safeguarded Copy* štiti podatke od sajbernapada pomoću nepromenljivih, izolovanih kopija koje se ne mogu menjati ili brisati, ali se mogu brzo vratiti kako bi se podržao oporavak.

Moćan hardver

U hardverskom smislu posmatrano, najvažnije specifikacije IBM FS7300 storidž sistema su sledeće:

- Maksimalni *bandwidth* (čitanje): 50 GBps.
- Vreme odziva (čitanje): <50 µs.
- Maksimalni efektivni kapacitet u osnovnoj 2U šasiji: 2,2 PB.
- Procesor/PCIe Gen: *Intel Cascade Lake*, Gen 3 PCIe.
- Maksimalni broj *front-end* host portova: 24.
- Podržani kapaciteti IBM *FlashCore* modula: 4,8 TB, 9,6 TB, 19,2 TB i 38,4 TB.
- Podržani kapaciteti drajvova *Storage class memory*: 1,6 TB.

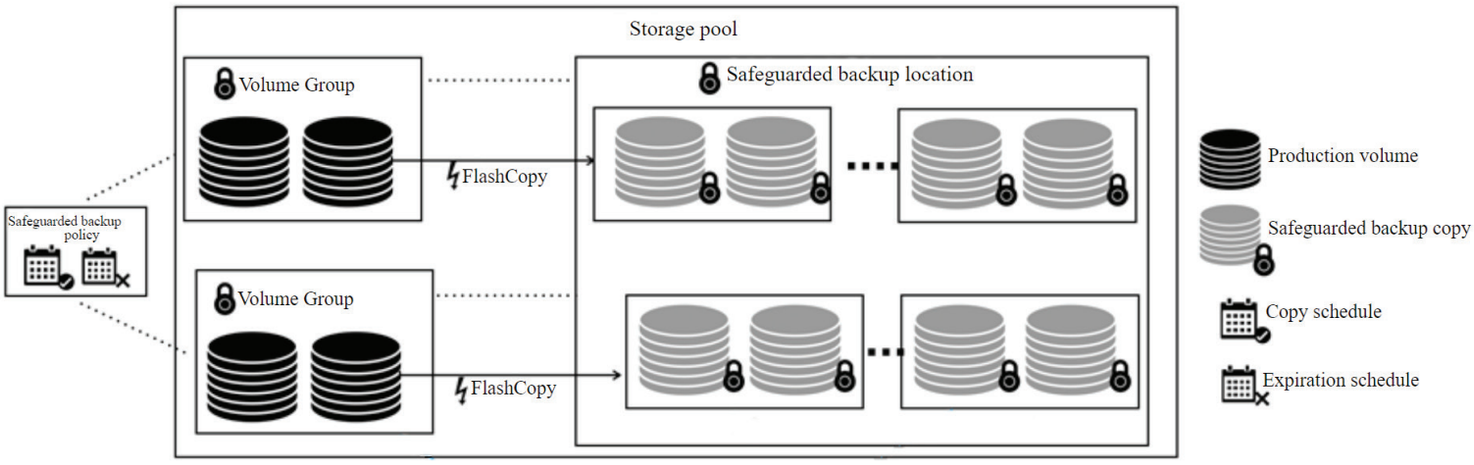
Model IBM *FlashSystem* FS9500 poseduje sledeće hardverske karakteristike:

- Maksimalni *bandwidth* (čitanje): 100 GBps.
- Vreme odziva (čitanje): < 50 µs.
- Maksimalni efektivni kapacitet u osnovnoj 4U šasiji: 4,5 PB.
- Procesor/PCIe Gen: *Intel Ice Lake*, Gen 4 PCIe.
- Maksimalni broj *front-end* host portova: 48.
- Podržani kapaciteti IBM *FlashCore* modula: 4,8 TB, 9,6 TB, 19,2 TB i 38,4 TB.
- Podržani kapaciteti drajvova *Storage class memory* (SCM): 1,6 TB.

IBM FS7300 i FS9500 storidž sistemi su idealno rešenje za korišćenje u okruženjima kao što su: SAP, *Oracle*, serverska i desktop virtuelizacija, produkcione baze podataka i kontejnersko okruženje.

Jedan od najvećih izazova za kompanije je kako da iskoriste prednosti tehnologije hibridnog *cloud*-a bez troškova zamene tre-

Slika 2. – IBM FS9500



Slika 3. – Safeguarded Copy

nutnog storidž sistema. Softver IBM *Spectrum Virtualize,* koji pokreće IBM FS7300 i FS9500, omogućava korišćenje storidž prostora u *cloud*-u za oporavak od katastrofe (*Disaster Recovery* - DR), znatno ubrzava razvijanje hibridnih konfiguracija u *cloud*-u i doprinosi smanjenju troškova skladištenja.

Kombinovanjem IBM FS7300 i FS9500 sa IBM *Spectrum Virtualize for Public Cloud* otvaraju se novi načini za kreiranje hibridnih rešenja u *cloud*-u između lokalnih privatnih *cloud*-a i javnog *cloud*-a.

Takođe, omogućena je replikacija podataka u realnom vremenu i oporavak od katastrofe (DR), kao i migracija podataka između lokalnog storidž sistema i IBM *cloud*-a, *Amazon Web Services* (AWS) ili *Microsoft Azure*-a. Zahvaljujući svojoj softverski definisanoj prirodi skladištenja, IBM *Spectrum Virtualize* omogućava administraciju skladištenja na lokaciji dobavljača usluga u *cloud*-u na isti način kao i *on-premises*, bez obzira na vrstu skladišta.

Data resilience ili otpornost podataka

Prema podacima koji su izneti na Svetskom ekonomskom forumu (WEF), od 2008. do 2016. godine više od dvadeset miliona ljudi godišnje bilo je primorano da napusti svoje domove usled ekstremnih događaja, kao što su poplave, oluje i požari. Te katastrofe utiču i na poslovanje. Pored prirodnih katastrofa, prema WEF-u, sajbernapadi su sada jedan od deset najvećih dugoročnih rizika. Napadači koriste veštačku inteligenciju (AI) da osmisle sajbernapade, pa je tako izračunato da će jedna od četiri organizacije doživeti napad u naredne dve godine. Većina ispitanika u pomenutom istraživanju očekivala je povećanje rizika od sajbernapada koji će dovesti do krađe novca i podataka (75 odsto) i kvarova u IT infrastrukturi (76 odsto). *Financial Times* objavio je da su se napadi *ransomware*-a „dvostruke iznude“, tj. hakeri koji kradu i enkriptuju osetljive informacije na licu mesta, a zatim prete da će ih objaviti, povećali za 200 odsto u 2020. godini. Dok je srednja veličina „žrtve“ ostvarivala prihod od 40 miliona dolara, više od 100 „žrtava“ imalo je godišnji prihod veći od milijardu dolara.

Sa sajbernapadima, podaci se vrlo često inficiraju, ali detektovanje zlonamernog softvera može potrajati i više od šest meseci. Priprema za oporavak od ovakve situacije znači da bi trebalo posedovati rezervne kopije podataka dovoljno dugo vremena da bi se pronašla takva kopija koja nije inficirana.

Svakako, prvi zadatak je sprečiti napadače da dobiju pristup interesnim podacima. IBM je lider u industriji *security* rešenja koja su dizajnirana da zaustave narušavanje podataka pre nego što se dogode. Jedan od mehanizama zaštite koji se može uhvatiti ukoštac sa sve češćim sajbernapadima jeste IBM *Safeguarded Copy*.

Softver IBM Spectrum Virtualize, koji pokreće IBM FS7300 i FS9500, omogućava korišćenje storidž prostora u cloud-u za oporavak od katastrofe, ubrzava razvijanje hibridnih konfiguracija u cloud-u i doprinosi smanjenju troškova skladištenja

Mehanizam *Safeguarded Copy* (slika 3) podržava mogućnost kreiranja sajberotpornih *point-in-time* kopija koje se ne mogu promeniti ili izbrisati usled korisničkih grešaka, zlonamernih radnji ili napada *ransomware*-a. Sistem se integriše sa IBM *Copy Services Manager*-om kako bi obezbedio automatizovane rezervne kopije i oporavak podataka. IBM *Copy Services Manager* koristi *Safeguarded* polise da automatski konfiguriše *FlashCopy* mapiranje i grupe za kreiranje rezervnih kopija.

IBM *Copy Services Manager* ispituje sistem svakih pet minuta kako bi obradio postojeće *Safeguarded* polise. Početno vreme koje je definisano u *Safeguarded* polisi mora da uračuna moguće kašnjenje od pet minuta. Kada IBM *Copy Services Manager* otkrije novu *Safeguarded* polisu za grupu volumena, kreira sesiju i definiše zadatak za kreiranje i upravljanje zaštićenim rezervnim kopijama.

Mehanizam *Safeguarded Copy* odvaja rezervne kopije od produkcionih podataka, tako da ukoliko dođe do nekog sajbernapada, mogu se brzo oporaviti i vratiti podaci sa tih rezervnih kopija (*backup*-a).

Po istraživanju *Proofpoint*-a iz 2020, 88% kompanija je u 2019. doživelo *phishing* napad. Kompanije mogu da smanje sajbernapade pomoću efikasnog sistema sajberbezbednosti koji za cilj ima da spreči, otkrije i prijavi sajbernapade koristeći ključne tehnologije sajberbezbednosti i najbolje prakse.

Kako bi se ostvario kontinuitet poslovanja, IBM redovno ažurira svoj hardverski i softverski portfolio, upravo zbog velikog broja sajbernapada, a jedan od vodećih sistema u ovoj oblasti su i IBM *FlashSystem* storidž uređaji i napredni IBM *Safeguarded Copy* softver.

➔ ***ComtradeDistribution.rs***

Najsigurnije mesto za vašu IT opremu

Trend razvoja Data centara je na globalnom nivou u stalnom porastu jer većini organizacija ovakav način čuvanja i obrađivanja podataka postaje prvi izbor, zbog niza prednosti koje nudi. Korisnik data centra može sa bilo kog mesta na svetu i koristeći bilo koji uređaj za pristup mreži, da radi sa potrebnom i dovoljnom računarskom snagom, potrebnom količinom memorije, neophodnim softverom i da podatke sigurno skladišti.

Data centar **A1**, koji postoji od 2012. godine, nudi mogućnost kompanijama da povećaju dostupnost, pouzdanost i kvalitet servisa koje pružaju zaposlenima i krajnjim korisnicima, da zaštite svoje poslovanje implementacijom BC i DR plana, i izbegnu krupne investicije kao što bi bila izgradnja sopstvenog *data* centra. Čuvanje IT opreme obezbeđeno je uz poštovanje rigorozne svetske standardizacije TIER 3.

Pristup *data* centru moguć je u svakom trenutku samo ovlašćenom osoblju korisnika i na osnovu strogih internih procedura. Objekat se u potpunosti prati spolja i iznutra sistemom video-nadzora. Poseduje najmoderniji sistem kontrole pristupa sa specifičnim klasama koje zavise od potreba i u potpunosti je čuvan, sa 24/7 tehničkom podrškom i bezbednosnom službom. Korisnicima pruža maksimalan komfor uz poseban prilaz za utovar i istovar opreme, teretni lift, prostoriju za otpakivanje i montažu opreme, uslužni kancelarijski prostor, ali i uslugu *remote hands*.

Redundansa čuva podatke

Data centar ima više nezavisnih ulaza optičkih kablova, kao i raznovrsne nacionalne i međunarodne optičke veze, a mogućnošću stvaranja redundantnih trasa i nezavisnog Internet *upstream* povezivanja s *Telekom Austrija grupom* i svim većim POP lokacijama.

Objekat je projektovan i izgrađen na način da se obezbedi snabdevanje električnom energijom u skladu s najvišim industrijskim standardima, a napaja se električnom energijom preko dve nezavisne trafo-stanice. Svaka linija je povezana sa sopstvenom transformator-stanicom koja opslužuje 1 MW električne energije.

Lociran u industrijskoj zoni Kragujevca, nedaleko od magistralnog puta, zauzima površinu od 1500 m^2.

U ponudi je smeštanje opreme u okviru deljenog ormana na nivou zakupljenog *unit*-a, a korisnici mogu zakupiti i cele ormane, u zavisnosti od potreba.

Stalni nadzor

Building Management System omogućava praćenje bezbednosnih aspekata, električnih instalacija, termotehničkih sistema, temperature, vlažnosti vazduha... Sistem za hlađenje realizovan je u konfiguraciji N+1, UPS sistem u konfiguraciji N+N, i dizel-generator u konfiguraciji N+1. Restriktivan pristup objektu georedundansa, odsustvo negativnih uticaja trusnog područja i blizine vode, kao i sve prethodno navedeno, samo su neke od vrednosti koje je potrebno istaći.

U okviru *A1 data centra* omogućene su usluge nacionalnog i međunarodnog povezivanja i pristup Internetu s tri nezavisna optička privoda. Ključna karakteristika za opredeljenje korisnika je najviši nivo kvaliteta, uz najpovoljnije tržišne uslove i ponuda prilagođena zahtevima korisnika.

Dodatno, korisnicima *data* centra će uskoro biti dostupna i usluga čuvanja podataka. *Back up as a service* je rešenje koje nudi brzo, jednostavno i automatizovano skladištenje sigurnosnih kopija podataka s korisničke infrastrukture na servere *A1 data centra*.

→ *A1.rs*

Da li je data centrima potrebna antivirus zaštita?

Nije, ako data centar držite pod staklenim zvonom, bez razmene podataka i fizičke veze sa njim. U tom slučaju vam ne treba ni data centar

Denis Daničić, Inženjer tehničke podrške, Extreme d.o.o.

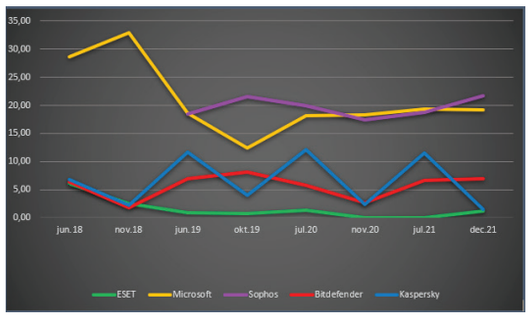
Šalu na stranu, ali iza ovog pomalo banalnog i čestog pitanja zapravo se krije briga administratora da će antivirus nekako da „pobrka lončiće“ u najvažnijem i najosetljivijem delu mreže.

Da li će antivirus usporiti servere?

U određenoj meri sigurno jer kao i svaka druga aplikacija i antivirus troši neke resurse. S jedne strane bezbednost nema alternativu, a sa druge performanse ne smeju biti ugrožene. ESET u svojim proizvodima isporučuje i jedno i drugo, pa je kroz trideset godina razvoja postao sinonim za efikasnost i brzinu rada uz minimalni utrošak sistemskih resursa. Optimizacija njegovog *Treath Sense* endžina je do te mere usavršena da u virtuelnom okruženju, sa ESET instalacijama na velikom broju mašina, hostovi ne pokazuju bitnije znake umora niti tragove „antivirusnih oluja“. U prilog tome govori i najava obustave daljeg razvoja *agentless* zaštite za *VMware* jer *VMware Tools* troši podjednako kao i ESET *Server Security*. ESET *Shared Local Cache* za optimizaciju skeniranja u lokalu diskontinuiran je prošle godine jer više nema potrebe za njim. ESET *Server Security* sa svojim tehnologijama, uz ESET servise u oblaku, ima najbolje performanse u branši.

Da li će raditi sve aplikacije?

Ako su u pitanju servisi globalnih proizvođača softvera, a vi ažurno održavate svoje instance, neće biti problema. Neažurne sisteme i aplikacije ESET neće kočiti u radu, ali ni stepen bezbednosti neće biti isti. Vi gradite i održavate tvrđavu, a ESET brine o njenoj odbrani. Ako u poslovanju koristite lokalne aplikacije koje ponekad biju bitku sa antivirusima, ni tu nema prevelike brige – sve radi kad se dobro podesi. ESET *Server Security* u toku instalacije pravi automatsku listu izuzetaka za *Microsoft* servise i podrazumevane i prilagođene lokacije resursa koje koriste. Za specifične aplikacije izuzetke možete kreirati po lokaciji, tipu fajla, procesu, hešu, protokolu, adresi, pa čak i virusnoj detekciji ukoliko je potrebno. U nekoliko klikova polise se šalju na sve mašine u data centru, čak i pre instalacije klijenta zaštite. Ne treba zaboraviti i na podršku da se do željenog rešenja dođe, a na par hopova je i direktna pomoć proizvođača.



Grafikon opterećenja sistemskih resursa (manje je bolje) / Izvor: AV Comparatives

Da li je ESET Server Security dovoljna zaštita za data centar?

Uz preporučene mere koje će uskoro izlaziti iz frižidera, obavezno ažuriranje operativnog sistema, aplikacija i redovno pravljenje funkcionalnih rezervnih kopija, ESET *Server Security* će obezbediti brzu i efikasnu zaštitu data centra, bez primetnog gubitka na performansama. U većini slučajeva to je dovoljno, ali nije sve što ESET nudi.

XDR za dodatnu sigurnost

U svetlu aktuelnog trenda razvoja ciljanih pretnji koje se pre napada, a to najčešće čine ransomverom, vešto prikrivaju i mesecima prikupljaju podatke o sledećoj žrtvi, treba razmisliti i o integraciji kvalitetnog XDR (*Extended Detection and Response*) rešenja. **ESET Protect & Inspect Cloud** (EPIC) će vam omogućiti da zavirite u najskrivenije odaje data centra u potrazi za sumnjivim aktivnostima. U EPIC konzoli sve je kao na dlanu – ko se ubacuje u legitimne procese, ko zakazuje nove zadatke, ko preuređuje registre i startne sekvence, ko manipuliše podešavanjima, ko koristi nestandardne kanale za komunikaciju itd. Administratoru preostaje da kroz ugrađena ili novokreirana pravila i izuzetke definiše bezbednosne okvire svoje mreže.

Održivi pristup za izvesnu budućnost

U želji da u zaključku dovoljno naglasim očigledno, jedna misao mi ne izlazi iz glave. Podatak da data centri širom sveta, od digitalnih zaseoka do grandioznih megalopolisa, troše 1-2% globalne proizvodnje električne energije u meni izaziva i divljenje i strah. I srećan sam jer kompanija koju zastupam insistira upravo na očuvanju resursa, kako digitalnih, tako i onih prirodnih koji su za apetite civilizacije veoma ograničeni. Bilo bi zanimljivo izračunati koliko je ESET za sve ove godine uštedeo struje na planeti. Dok čekamo taj podatak na nama je da budemo štedljivi, efikasni i praktični. I budimo realni – u pola godine naš Exchange imao je 380 unikatnih napada i nijedan prolaz. Antivirusna zaštita mora da postoji.

→ *Extreme.rs*

Zaštita podataka

Bezbednost podataka nije vezana samo za njihov integritet i poverljivost, već i za potrebu da oni budu uvek dostupni. Poslovi registracije naziva domena uključuje prikupljanje i korišćenje različitih vrsta podataka i stoga RNIDS svoju dužnost i obavezu zaštite podataka klijenata shvata veoma ozbiljno

Žarko Kecić

Sajber kriminal je u porastu, a priroda i složenost napada stalno evoluiraju, pri čemu se kriminalci oslanjaju na nova sofisticirana sredstva napada da bi ostali ispod radara i kompromitovali mreže korisnika koji ništa ne sumnjaju. Hakovanje sistema i krađa podataka za preprodaju, ucene ili zloupotrebu na neki drugi način, prema procenama stručnjaka, sajber kriminalcima donosi godišnji prihod od oko 1,5 biliona dolara. Ovakvi incidenti se uglavnom događaju zbog nepažnje i neadekvatnih mera zaštite onih koji ove podatke prikupljaju i čuvaju.

Bezbedan i stabilan

Najbolji opis ključnih servisa RNIDS-a u par reči, bilo bi „bezbedan i stabilan“. Ponosni smo što možemo da kažemo da se obe reči odnose na naše upravljanje nacionalnim internet domenima (.rs i .срб) u Srbiji. Naša industrija suočava se sa nizom sajber pretnji i naš zadatak je da upravljamo i održavamo infrastrukturu koja omogućava da sve usluge i sadržaji koji su vezani za te domene, budu stalno dostupni i vidljivi na Internetu.

Bezbednost podataka nije vezana samo za njihov integritet i poverljivost, već i da oni budu uvek dostupni kada je to potrebno. Poslovi registracije naziva domena uključuje prikupljanje i korišćenje različitih vrsta podataka i stoga RNIDS svoju dužnost i obavezu zaštite podataka naših klijenata shvata veoma ozbiljno. To ne podrazumeva samo zaštitu ličnih i poslovnih podataka od krađe, već i zaštitu integriteta podataka koji omogućavaju da sistemi i servisi naših klijenata budu neprekidno vidljivi na internetu.

Da bi ispunili ciljeve koji se od RNIDS-a očekuju, bilo je potrebno investirati u robusnu i stabilnu infrastrukturu i mnogo truda da se definišu pravila i procedure koje obezbeđuju:

- **Tajnost podataka** – preduzimanje potrebnih mera da podacima ne mogu pristupiti neautorizovane osobe;
- **Integritet podataka** – obezbediti da podaci u sistemima RNIDS-a budu tačni i potpuni;
- **Raspoloživost** – osigurati da servisi i podaci budu stalno dostupni.

Aktivnosti RNIDS-a podrazumevaju svakodnevno prikupljanje i obradu različitih vrsta podataka koji imaju različite zahteve po pitanju bezbednosti. Poslovni i lični podaci o kontaktima vezanim za nazive domena moraju biti zaštićeni od krađe i

zloupotrebe, dok su DNS podaci javno dostupni, ali bi njihove neovlašćene izmene mogle da prouzrokuju ozbiljnu štetu korisnicima.

RNIDS je svoju opremu i servise smestio u data centre koji ispunjavaju visoke standarde fizičke i tehničke zaštite uređaja i podataka koji se nalaze na njima: 24/7 fizičku zaštitu, redundantne sisteme neprekidnog napajanja, redundantnu kontrolu temperature i vlažnosti, kao i zaštitu od požara, poplava i zemljotresa

Infrastruktura koja omogućava visoku raspoloživost

Za realizaciju zahteva vezanih za bezbednost podataka i implementaciju odgovarajućih pravila i procedura potrebno je obezbediti i kompleksne tehničke uslove, koji nisu vezani samo za kontrolu i ograničenje prava pristupa IT sistemima RNIDS-a već podrazumevaju i fizičku zaštitu uređaja, obezbeđenje neprekidnog napajanja električnom energijom, obezbeđenje optimalnih uslova za rad opreme, kao i obezbeđenje nastavka poslovnih aktivnosti u slučaju prirodnih katastrofa i sličnih događaja.

Da bi svi ovi zahtevi bili u potpunosti ispunjeni, RNIDS je svoju opremu i servise smestio u *data* centre koji ispunjavaju visoke standarde fizičke i tehničke zaštite uređaja i podataka koji se nalaze na njima. *Data* centri u kojima je smeštena oprema RNIDS-a imaju 24/7 fizičku zaštitu od neovlašćenog pristupa, redundantne sisteme neprekidnog napajanja, redundantnu kontrolu temperature i vlažnosti, kao i odgovarajuću zaštitu od požara, poplava i zemljotresa.

Vrhunski *data* centri ipak nisu dovoljna garancija da će servisi i podaci uvek biti dostupni i bezbedni. Uspostavljanje redundantne infrastrukture na kojoj se nalaze ključni servisi RNIDS-a predstavljalo je dugotrajan proces planiranja, odabira odgovarajuće tehnologije, implementacije i testiranja, što kao rezultat ima veoma stabilan sistem, otporan na kvarove i neočekivane ispade njegovih pojedinih delova. Time je omogućeno da sistem za registraciju naziva domena radi sa više aktivnih instanci, na različitim lokacijama.

Takođe, implementirane bezbednosne mere ovom sistemu implementiraju višestruke kontrole pristupa i bezbedan prenos podataka između RNIDS-a i svih učesnika procesa registracije naziva domena. Na taj način, osim visoke dostupnosti, obezbeđen je i visok stepen zaštite podataka koje RNIDS prikuplja i obrađuje.

Zaključavanje i zaštita domena

Zbog načina na koji se sprovodi proces registracije naziva domena, ipak postoje minimalne šanse za kompromitaciju i neautorizovanu izmenu podataka. RNIDS je iz tog razloga svojim korisnicima stavio na raspolaganje nekoliko opcija za zaključavanje i zaštitu domena. RNIDS svim korisnicima savetuje da iskoriste ove bezbednosne mere, pogotovo ako se uzme u obzir da se dva od tri načina zaključavanja dodatno ne naplaćuju.

Ipak, najznačajnija usluga RNIDS-a je DNS servis koji omogućava ispravan i neprekidan rad .rs i .срб naziva domena. DNS je osnovni internet servis koji omogućava komunikaciju na internetu i kao takav je stalna meta napada kriminalaca. Prema navodima vodećih kompanija za bezbednost, skoro dve trećine svih sajber napada izvedeno je nekom vrstom manipulacije DNS-a. RNIDS ima posebnu odgovornost da ovaj servis za srpske nacionalne domene radi besprekorno, jer bi u suprotnom svi *Web* sajtovi i ostali internet servisi na .rs i .срб domenima bili nedostupni, a korisnici ne bi mogli da razmenjuju elektronsku poštu. Iz tog razloga, RNIDS je razvio globalnu mrežu DNS servera koja je omogućila da više od deset godina ovaj servis radi bez prekida i da korisnicima .rs i .срб možemo da garantujemo stoprocentnu dostupnost i ubuduće.

Osim visoke dostupnosti DNS servisa, RNIDS omogućava i upotrebu savremenih bezbednosnih proširenja DNS-a, tj. uspostavljanje lanca poverenja za kriptografsko potpisivanje DNS zapisa, poznatije kao DNSSEC. Na taj način onemogućava se bilo kakva neautorizovana izmena DNS zapisa i preusmeravanje korisnika na internet lokacije koje kontrolišu sajber kriminalci.

Najčešća vrsta napada kojoj su izloženi svi korisnici interneta, a mnogi i nasednu na primamljive ponude prevaranata, su fišing *(phishing)* napadi, tj. pokušaji da se nepažljivi korisnici navedu da se radi o poruci koja je stigla od kredibilne institucije i ostavljaju svoje lične i osetljive podatke. Iz tog razloga, RNIDS vodi računa i da minimizuje količinu sadržaja koji služi za prevaru ili širenje zlonamernih programa na .rs i .срб domenima.

Uz pomoć DNS-a mogu se prepoznati obrasci i trendovi koji ukazuju na zlonamerno ponašanje. Koristeći ove podatke u stanju smo da identifikujemo domene koji imaju sadržaje opasne po korisnike i da relativno brzo reagujemo u cilju njihovog uklanjanja.

Na žalost, sajber kriminalci konstantno unapređuj metode i tehnike koje im omogućavaju krađu i zloupotrebu podataka. Iz tog razloga, iako su bezbednost podataka i dostupnost servisa RNIDS-a na veoma visokom nivou, naš zadatak je da svakodnevno pratimo savremene trendove u ovoj oblasti, razmenjujemo iskustva sa drugim registrima u svetu i unapređujemo naše sisteme u cilju povećanja bezbednosti naših korisnika i zaštiti njihovih podataka.

→ *rnids.rs*

RNIDS omogućava uspostavljanje lanca poverenja za kriptografsko potpisivanje DNS zapisa, poznatije kao DNSSEC. Na taj način onemogućava se neautorizovana izmena DNS zapisa i preusmeravanje korisnika na internet lokacije koje kontrolišu sajber kriminalci

Analiza rizika

Procena potreba

Optimizacija investicija

Projektovanje

Implementacija

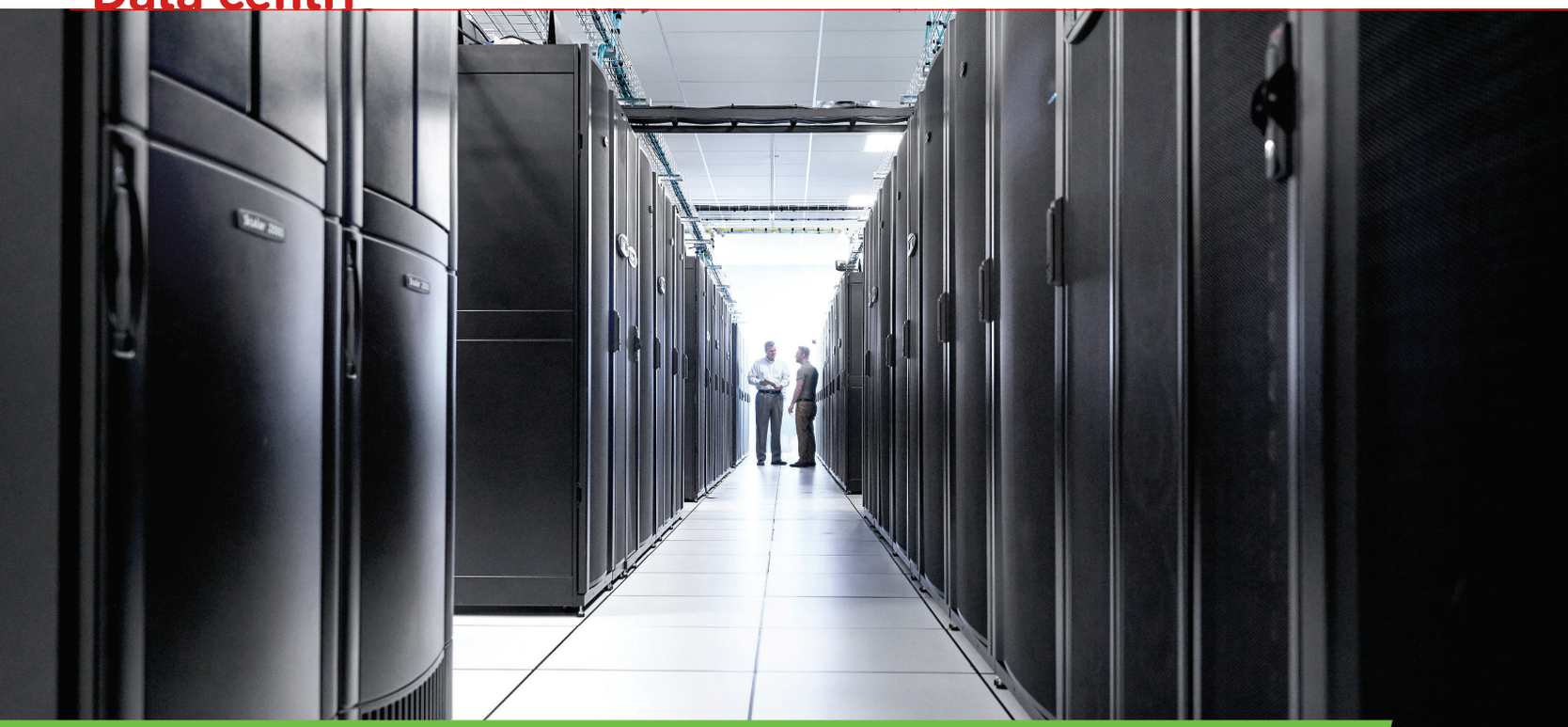
Održavanje

Podrška

godina iskustva

ČEKAMO VAS

RITTAL



Fizička bezbednost data centara

Današnje uobičajene tehnike za praćenje okruženja data centra datiraju iz vremena centralizovanih mejnfrejmova i uključuju prakse kao što su hodanje s termometrima i oslanjanje na IT osoblje kako bi „osetili“ okruženje u prostoriji

Dušan Ćirić, Product Application Engineer – Secure Power

Budući da *data* centri nastavljaju da se razvijaju s distribuiranom obradom (*edge*) i naprednim serverskim tehnologijama koje iziskuju sve veće potrebe za strujom i hlađenjem, ambijentalni uslovi i bezbednost okoline moraju se detaljnije razmatrati. Rastuća gustina snage i dinamičke varijacije snage su dva glavna pokretača koji nameću promene u metodologiji praćenja IT okruženja.

Nadzor opreme nije dovoljan – okruženje mora biti posmatrano holistički, a bezbednosne pretnje i upadi prepoznati i proaktivno sprečeni. Takve pretnje uključuju previsoke temperature na ulazu servera, curenje tečnosti i neovlašćeni pristup ljudi ili neodgovarajuće radnje osoblja u *data* centru.

Pod stalnim nadzorom

Udaljene lokacije, kao što su server sale „na ivici“, filijale i lokacije s rekovima mrežne koncentracije, sve veći broj lokacija bez osoblja, dodatno nameću potrebu za automatizovanim nadzorom. S današnjim tehnologijama, sistemi za praćenje se mogu konfigurisati do nivoa detalja koji ispunjava posebne ekološke i bezbednosne zahteve *data* centra – svaki rek može biti smatran mini – *data* centrom sa sopstvenim zahtevima, sa strategijom praćenja koja može uključiti više tačaka za prikupljanje podataka.

NetBotz linija proizvoda kompanije *Schneider Electric* pomaže korisnicima da daljinski upravljaju ambijentalnom i fizičkom bezbednošću opreme:

- Senzori mogu da prate temperaturu, vlažnost i pojavu tečnosti i šalju upozorenja;
- kamere mogu da prate fizičku bezbednost IT opreme, obezbeđujući vizuelnu identifikaciju ulaska i izlaska;
- daljinskim upravljanjem postoji mogućnost praćenja daljinskog otvaranja i zatvaranja vrata, daljinski pristup reku preko ID kartice, pa čak i uključivanje i isključivanje povezanih utičnica.

NetBotz senzori i kontrola samo su jedan aspekt šire *EcoStruxure* softverske platforme za nadgledanje i upravljanje infrastrukturom. Rešenje je potpuno nezavisno od proizvođača opreme i nudi razne opcije za nadgledanje i upravljanje IT infrastrukturom na licu mesta (*on premise*), u oblaku (*on cloud*) i na ivici.

Spektar bezbednosnih pretnji

Pretnje po *data* centre mogu se klasifikovati u dve široke kategorije, u zavisnosti od toga da li su u domenu IT softvera i umrežavanja (digitalne pretnje) ili u domenu podataka infrastrukture za fizičku podršku *data* centra (fizičke pretnje).

Fizičke pretnje uključuju i probleme s napajanjem i hlađenjem, ljudske greške ili zlonamernost, vatru, curenje tečnosti i kvalitet vazduha. Neke od njih se rutinski nadgledaju standardnim, ugrađenim mogućnostima samih uređaja koji se prate, npr:

- UPS sistemi prate kvalitet struje, opterećenje i stanje baterija;
- PDU-ovi nadgledaju opterećenja strujnih kola;
- rashladne jedinice nadgledaju ulaz i izlaz temperature i status filtera;
- sistemi za gašenje požara prate prisustvo dima ili toplote.

Nadgledanje se realizuje prema dobro poznatim protokolima i automatizovanim softverskim sistemima koji agregiraju, evidentiraju, tumače i prikazuju informacije.

Određene vrste ozbiljnih fizičkih pretnji ne stavljaju se korisniku unapred na raspolaganje, kroz ugrađena rešenja za praćenje. Na primer, pretnja neadekvatnog nivoa vlažnosti može biti bilo gde u *data* centru,

tako da su broj i pozicioniranje senzora za merenje vlažnosti važan faktor u upravljanju tom pretnjom. Takve pretnje mogu potencijalno biti distribuirane bilo gde, i spadaju u sledeće opšte kategorije:

- Pretnje kvalitetu vazduha za IT opremu (temperatura, vlažnost);
- curenje tečnosti;
- ljudsko prisustvo ili neobična aktivnost;
- pretnje kvalitetu vazduha za osoblje (strane supstance u vazduhu);
- dim i vatra nastali iz nezgoda u *data* centru ili neposredno pored njega.

Različiti tipovi senzora se koriste za rano upozorenje i detekciju problema nastalih od navedenih pretnji. Postoji minimalni osnovni skup senzora koje treba implementirati u većini *data* centara: senzori temperature i vlažnosti, uže za detekciju curenja tečnosti ili tačkasti senzor za detekciju tečnosti, digitalne kamere.

Pored osnovnih senzora, postoje i opcioni, i tu spadaju senzori za detekciju: dima, pokreta, vibracija, otvorenosti vrata rek ormana. Napredni nivo fizičke zaštite može se postići i ugradnjom sistema za kontrolu pristupa na samim rek ormanima.

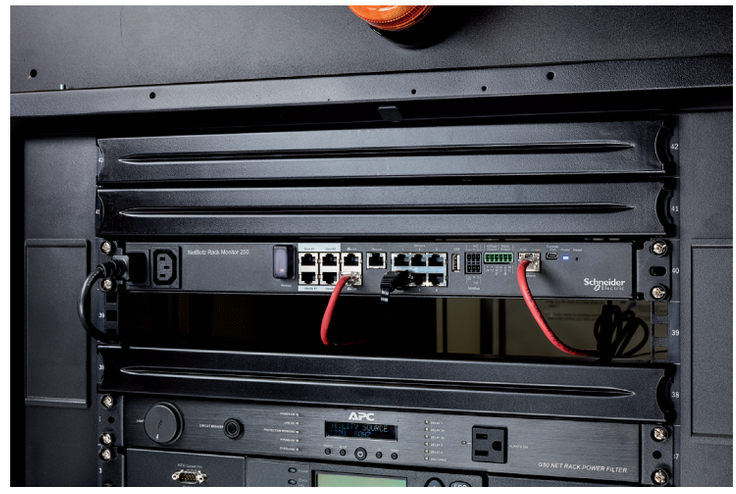
Centralizovan pregled data centra

NetBotz je najsveobuhvatnije rešenje u industriji praćenja bezbednosnih i ambijentalnih uslova kako bi IT oprema korisnika bila maksimalno zaštićena od pretnji iz okruženja u kome se nalazi ili ljudskih fizičkih pretnji.

Po odabiru i postavljanju senzora, sledeći korak je prikupljanje i analiza podataka koje senzori primaju. Umesto da se podaci sa senzora šalju direktno na centralnu tačku prikupljanja, obično je bolje imati tačke agregacije raspoređene po celom *data* centru, s mogućnostima upozorenja i obaveštavanja na svakoj tački. Ovakvim pristupom ne samo da se eliminiše rizik od kvara u jednoj tački za centralnu agregaciju već je pogodan i za nadgledanje udaljenih serverskih soba i telekomunikacionih rekova.

Pojedinačni senzori se kod *NetBotz* rešenja ne povezuju pojedinačno na IP mrežu. Umesto toga, agregatori tumače podatke senzora i šalju upozorenja centralnom sistemu i/ili direktno na listu za obaveštenja. Ova arhitektura distribuiranog nadzora drastično smanjuje broj potrebnih prekida mreže i smanjuje ukupne troškove sistema i opterećenje upravljanja. Agregatori se obično dodeljuju fizičkim oblastima unutar *data* centra, agregiraju senzore iz njih i takvom postavkom se smanjuje složenost ožičenja senzora.

Senzori obezbeđuju neobrađene podatke, ali podjednako je važna i interpretacija ovih



podataka kako bi se dala upozorenja, obaveštenja i korektivne mere. Budući da strategije praćenja postaju sve sofisticiranije, a senzori se umnožavaju kroz dobro nadgledani *data* centar, „inteligentna“ obrada ove potencijalno velike količine podataka je kritična. Najefikasniji način prikupljanja i analize podataka sa senzora i pokretanja odgovarajućih akcija jeste upotrebom takozvanog „agregatora“.

Neophodno je imati mogućnost filtriranja podataka, određivanja korelacija između njih i da se na osnovu toga izvrše procene kako bismo odredili najbolje akcije kada parametri idu van granica.

Fino podešen sistem

Dobro definisani pragovi alarma (graničnih vrednosti), metode obaveštavanja (kako i kome proslediti alarm) i eskalacije (različite vrste alarma) ključne su aktivnosti za uspostavljanje kvalitetnog i pouzdanog sistema za upozoravanje.

Zaštita od distribuiranih fizičkih pretnji ključna je za sveobuhvatnu bezbednosnu strategiju. Dok postavljanje i metodologija senzorske opreme zahtevaju procenu, odluku, dizajn, najbolje prakse i alati za dizajn su dostupni da pomognu u efikasnom raspoređivanju senzora. Pored odgovarajućeg tipa, lokacije i broja senzora, moraju biti implementirani i softverski sistemi za upravljanje prikupljenim podacima i obezbeđivanje evidencije, analize trendova, inteligentnog upozorenja obaveštenja i automatizovane korektivne mere gde je to moguće. *Schneider Electric* nudi kompletno rešenje koje obuhvata *NetBotz* platformu s pratećim senzorima i *EcoStruxure* IT softver za centralizovani nadzor svih tačaka i uređaja. Konstantnim i posvećenim ulaganjem u razvoj bezbednosti proizvoda i softvera, *Schneider Electric* svojim klijentima nudi bezbedna i pouzdana rešenja za nadzor.

Razumevanje tehnika za praćenje distribuiranih fizičkih pretnji omogućava IT administratorima da popune kritične praznine u ukupnoj bezbednosti *data* centra i da zadrže fizičku bezbednost usklađenu s promenljivom infrastrukturom *data* centra i ciljevima dostupnosti.

➔ ***ecostruxureit.com/netbotz/***

Vertiv™ VRC-S Edge-Ready micro data centar

Izgradite svoj edge data centar prema sopstvenim potrebama koristeći različite dostupne konfiguracije našeg novog mikro data centra

Vertiv™ VRC-S, potpuno fabrički sastavljen mikro *data* centar dizajniran za brzu i laku instalaciju na *edge* lokacijama, što bližim krajnjim korisnicima te ostalim manjim IT prostorima. Dostupan sada u Evropi, na Bliskom istoku i Africi (EMEA regija), *Vertiv*™ VRC-S inkorporira jedinicu za distribuciju energije (rPDU – *rack power distribution unit*), *Energy Star* 2.0 sertifikovani *Vertiv*™ *Liebert*® GXT5 neprekidni sistem napajanja (UPS), softver i senzore za monitoring, kao i najnoviji *Vertiv*™ VRC sistem hlađenja u visokoefikasnom IT ormaru koji pruža celovito rešenje.

Vertiv VRC-S dolazi s trogodišnjom garancijom koja pokriva ceo sistem

Višenamenska funkcionalnost

Mikro *data* centri dizajnirani su za podršku *edge computing* aplikacijama, što znači primenu kritičnih resursa u manjim IT prostorima gde god su potrebni. Za razliku od prefabrikovanih modularnih *data* centara, koji su tipično veće samostalne instalacije koje se koriste izvan glavne infrastrukture ili na udaljenim lokacijama, mikro *data* centri veličine standardnog IT ormara mogu biti iskorišćeni u različitim okolinama, kao što su kancelarije, klinike, prodavnice i ostali trgovački ili industrijski prostori. *Vertiv*™ VRC-S unapred je projektovan i fabrički integrisan kako bi pružio maksimalnu pouzdanost, efikasnost i brzinu postavljanja/instalacije.

Značajne karakteristike:

- *Edge* IT ormar dostupan u četiri standardne veličine.
- Unapred integrisana *Vertiv Geist* jedinica za distribuciju električne energije.
- *Vertiv* VRC rashladna jedinica omogućava kapacitet hlađenja do 3,5 kW.
- Integrisani ili razdelni sistem odbijanja toplote sve do nivoa od -15 °C ili -34 °C.
- Ugrađeni *Vertiv Intelligence Director* softver za monitoring, kontrolu i pristup svim komponentama na daljinu.
- Dostupne usluge instalacije.

Grejanje pod kontrolom

Kućište *Vertiv*™ VRC-S mikro *data* centra koristi poseban prolaz za hladan i topao vazduh unutar ormara za efikasan protok i prevenciju nagomilavanja toplote. Jedinica hlađenja montirana unutar ormara specijalno je osmišljena i dizajnirana za *edge computing* IT opterećenja. Koristeći kombinaciju ventilatora s promenjivom brzinom te kompresora varijabilne brzine, ova jedinica prilagođava kapa-

citet hlađenja prema stvarnoj disperziji IT toplote, što minimalizuje potrošnju energije. *Vertiv™ Liebert®* GXT5 *online,* visokoefikasni UPS sistem dvostruke konverzije, omogućava kontinuitet napajanja za sve integrisane komponente, uključujući 3,5 kW sistem za hlađenje i rezervnu ventilaciju. *Vertiv™ Geist™* rPDU omogućava distribuciju električne energije s upravljanjem na nivou utičnice i uključuje *Vertiv™ Inteligent Director* softver za upravljanje kako bi se omogućio daljinski monitoring i menadžment celog sistema napajanja i hlađenja kroz jedinstvenu IP adresu za jednostavno upravljanje opremom na daljinu, kao i prediktivno održavanje.

Dugotrajna podrška

Vertiv VRC-S dolazi s trogodišnjom garancijom koja pokriva ceo sistem. Instalacija i preventivne usluge održavanja dostupne su kroz *Vertiv* usluge servisa koje obezbeđuju lokalni i visokostručni profesionalci, kao i partneri.

„Izbor i primena mikro *data* centra nikada nije bila brža i lakša, a sada se može i virtuelno doživeti s novom aplikacijom proširene stvarnosti. *Vertiv* VRC-S je vrlo efikasno *plug and play* rešenje koje se može isporučiti na lokaciju s integrisanim UPS-om, koji napaja hlađenje unutar serverskog ormara i rezervnu ventilaciju u slučaju kvara, kao i distribuciju električne energije za IT sisteme s unapred postavljenim sistemom monitoringa za jednostavno spajanje s napajanjem i mrežom u vašem postrojenju. Ova nova ponuda je rezultat strateškog pristupa firme *Vertiv* koji se oslanja na inovativnost proizvoda te najnovijim R&D investicijama, koje će progresivno omogućiti više *edge-ready* mikro *data* centara tržištu“, izjavio je Ante Maršić, *Channel Sales Lead* za *Vertiv u CEE regiji.*

Kao idealno rešenje za namene u trgovinama i dostavama, transportu, zdravstvu i lakoj industriji, *Vertiv* VRC-S je dostupan u nekoliko verzija unapred konstruisanih standardnih modela koji mogu biti dostavljeni u najbržem mogućem roku, kao i instalirani za samo nekoliko sati.

Mikro data centar može se isprobati virtuelno Vertiv XR aplikacijom

VR pogled na sistem

VRC-S mikro *data* centar može se isprobati i virtuelno putem najnovije *Vertiv* XR aplikacije za pametne telefone na temelju proširene stvarnosti. *Vertiv* XR aplikaciju možete preuzeti s *Google Play* prodavnice (*Android*) i *Apple* prodavnice (iOS).

Ova aplikacija omogućava kupcima istraživanje svih komponenti jedinice, dok se u isto vreme otkrivaju načini rada i ključne osobine koje nisu vidljive golim okom, donoseći celoviti sistem funkcionalnosti koji je jedinstven na tržištu.

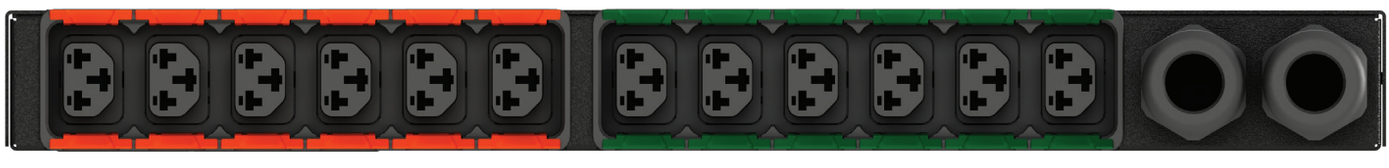
Sve što treba da učinite jeste da odaberete rešenje koje vam se čini najinteresantnijim, postavite realističan 3D model po želji ili potrebi, a potom istražite svaku njegovu komponentu u detalj, osetite njenu teksturu, prošetate oko nje kako biste otkrili sve njene mogućnosti i to iz svakog ugla.

Besplatno preuzmite *Vertiv™* XR i iskusite svoju buduću digitalnu infrastrukturu kao nikad do sada. Bićemo uvek samo jedan dodir ekrana udaljeni od vas i spremni za pomoć kako biste maksimalno iskoristili svoje kritične sisteme.

Više informacija o tome kako AR iskustvo pomaže u demonstraciji *Vertiv* VRC-S mikro *data* centra možete pronaći na *Vertiv Web* stranici. *Vertiv* je u Srbiji zastupljen preko ovlašćenih distributera *Kim Tec* i *Ingram Micro.*

➔ *Vertiv.com*

Mikro data centri mogu biti iskorišćeni u različitim okolinama, kao što su kancelarije, klinike, prodavnice i industrijski prostori




EDGE
Data
Centri
SVE IZ JEDNE RUKE
Vesimpex
Patrijarha Dimitrija 24, 11090 Beograd,
tel. 063 33 90 90
• www.itinfrastruktura.rs
• www.vesimpex.rs
• info@vesimpex.rs
RITTAL