PC PRESS

Backup **obavezno!**

Specijalni dodatak časopisa PC Press #280

Backup od 10 miliona dolara

Pratili ste nevolje kompanije Garmin: ruski hakeri uspeli su da im podmetnu ransomware koji je kriptovao podatke i onesposobio sve servise na gotovo nedelju dana. Najzad je Garmin morao da plate ucenu od (priča se) 10 miliona dolara da bi se sve vratilo u normalu. Zar firma te veličine ne pravi backup? Učimo se na njihovim greškama, jer su i naši podaci podložni napadima i havarijama...

Dejan Ristanović

Pomisliti da kompanija kao što je *Garmin*, čija je trenutna kapitalizacija oko 20 milijardi dolara i koja zapošljava 13.000 ljudi širom sveta, nema ozbiljno IT odeljenje sposobno da napravi tako običnu stvar kao što je *backup* zvuči jeretički, ali su događaji pokazali da je tako. Jer, da su imali upotrebljiv *backup*, teško da bi na svoju reputaciju stavili takvu mrlju kao što je plaćanje ucenjivaču. Da, svakako su pravili *backup*, ali cinična poslovica kaže da se firme dele na one koje nemaju *backup* i one koje misle da imaju *backup*...

Podaci i backup – nikad zajedno

Slična nevolja snašla je i Javno komunalno preduzeće „Informatika“ iz Novog Sada, kome su hakeri 1. marta ove godine blokirali sve podatke, između ostalog i o računima izdatim građanima kao i uplatama od strane građana. Traženo je 50 bitkoina ili oko 400.000 evra da se podaci otključaju, a pošto Novi Sad nije želeo da plati ucenu (gest koji u svakom slučaju podržavamo!), ostalo im je da prekucavaju podatke sa papirnih izveštaja. Posle toga je nastupila epidemija pa se o ovom problemu nije mnogo govorilo, ali svakako je to bila velika nevolja koja i do sada ostavlja neke tragove.

Ključni problem u oba slučaja bio je u tome što su aktivni računari imali pristup diskovima na kojima se pravi *backup*, dakle onaj ko „osvoji“ neki server u mreži može da zaključa ne samo osnovne podatke, nego i njihovu kopiju. Korisnik ostaje sa dve jednako beskorisne gomile bajtova, a originalne podatke nema nigde – *backup* je u pravom smislu te reči imaginaran.

Ispravan (ili makar ispravniji) način za organizovanje *backup*-a opisali smo u tekstu „Nezvani gost u Redakciji“ iz PC#265 – kada nas je *ransomware* pogodio, izgubili smo jedan dan dok smo reinstali-

rali server i vratili podatke sa *backup*-a, i to je bila sva šteta. Preporučujemo da pročitate taj tekst, a ovde ćemo samo ukratko reći da računari koji prave *backup* treba da imaju pristup diskovima sa podacima, ali računari koji obrađuju podatke **nikako** ne smeju imati pristup diskovima na kojima je *backup*. Dakle, kopiranje podataka na bezbedno mesto **ne** obavlja računar koji te podatke obrađuje, već drugi računar (ili NAS) koji je zadužen za *backup*. Da bi takav protokol funkcionisao, treba rešiti problem sa bazama koje su stalno otvorene pa se ne mogu tek tako prekopirati, ali svaki *data base* sistem *(Microsoft SQL Server, Oracle, MySQL...)* ima mehanizam kojim se baza stavlja u režim za *backup*, a nove transakcije se posebno beleže da bi, kada *backup* bude završen, bile ugrađene u samu bazu.

Dodajmo da ni ovakav scenario nije dovoljno bezbedan – on ne štiti od nesreće koja bi fizički uništila čitav hardver (zemljotres, požar...), kao ni od nekih sistemskih greški koje bi ipak dopustile da se prodre u *backup* sistem tako što se i on hakuje. Zato je neophodno da se *backup* povremeno (u slučaju važnih podataka dnevno ili češće) kopira na još jedan set medija koji se isključuju iz mreže i nose na drugu, sigurnu lokaciju, pa deponuju u tamošnji sef. Važni podaci se mogu arhivirati i preko Interneta prenositi na servere koji se nalaze u drugoj državi ili čak na drugom kontinentu.

Računari koji obrađuju podatke nikako ne smeju imati pristup diskovima na kojima je backup. Kopiranje podataka na bezbedno mesto ne obavlja računar koji te podatke obrađuje, već računar zadužen za backup

Serveri kao kućni ljubimci... ili kao stado

Opisana procedura je smislena u kućnoj kancelariji ili manjoj firmi gde su podaci jedino što treba sačuvati. Kada nas je pogodio *ransomware*, prosto smo formatirali disk, ponovo instalirali *Windows Server*, kreirali korisnike (ovoga puta sa jačim lozinkama) vratili podatke i nesmetano nastavili posao. Ali šta bi bilo da smo, što je svakako *Garmin*-ov slučaj, poslovanje zasnovali na stotinama servera širom sveta, na kojima su instalirani razni servisi koji međusobno komuniciraju? Super, podaci su sačuvani, ali kako je sav korišćeni softver instaliran i konfigurisan, kako su podešena prava, šta je u kom aktivnom direktorijumu, kako se pristupa podacima u oblaku... Teško da tu može da se krene od instaliranja softvera na svakom od servera, pa da se sačeka *update* (koji često traje duže od instalacije), pa da se onda stvari polako podešavaju i testiraju... trajalo bi mesecima.

Zanimljiva izreka, koja se (doduše u nešto drugačijem kontekstu) pripisuje Bilu Bejkeru *(Bill Baker)* iz *Microsoft*-a, kaže da servere treba tretirati kao stado, a ne kao kućne ljubimce *(treat servers as cattle, not pets)*. Ako administrator treba posebno da konfiguriše neki server i da se njime bavi, on ga tretira kao „kućnog ljubimca“, što znači da pokretanje tog servera zahteva mnogo više vremena i ljudskog rada nego što je neophodno, a podložnije je i greškama jer nije lako zapamtiti karakteristične potrebe svakog „ljubimca“. Osnovna konfiguracija svih servera treba da bude što sličnija, a softver koji se instalira i servisi koji se pokreću da budu zabeleženi u skriptove koji automatizuju proceduru. Kada server treba zameniti, zbog kvara, napada malicioznog softvera, prelaska na jaču hardversku konfiguraciju ili bilo kog drugog razloga, uzme se novi računar, pokrene skript i sve automatski dolazi u željeno stanje, a server je posle te automatizovane procedure spreman da se uključi u mrežu praktično bez čovekove intervencije.

Sve ovo je lako reći, a nije preteško ni realizovati pošto svi serverski operativni sistemi omogućavaju kreiranje automatskih instalacionih procedura (u *Linux* svetu se za upravljanje konfiguracijama često koristi alat *Ansible*, dok je *Microsoft* je od toga napravio čitavu nauku), ali zahteva kasniju disciplinu – kada se u konfiguraciju servera unesu neke izmene, treba ih ugraditi i u skriptove za automatsku instalaciju servisa. Važne su i povremene probe koje će pokazati da li skript i dalje automatski kreira adekvatno konfigurisan server. Obično se takve probe vrše na virtuelnim mašinama, da bi se smanjili zahtevi za fizičkim hardverom, a samim tim i troškovi.

Sistem otporan na otkaze

Kao što se nikada ne može napisati (netrivijalni) softver koji je potpuno lišen bagova ili konfigurisati računar tako da bude potpuno otporan na napade zlonamernih hakera, tako se ne može napraviti ni sistem potpuno otporan na otkaze. To ne znači da je trud uložen u kreiranje sigurnog sistema uzaludan – stvar je kompromisa koliko ćete rada, znanja i novca uložiti u otpornost sistema. Što više uložite, bićete bezbedniji i lakše ćete se oporaviti posle eventualne havarije ili napada.

Počnimo od nekih osnovnih smernica. Pre svega, ne smete imati ni jedan servis koji se izvršava na samo jednom računaru – bilo kakva havarija tog računara bi onesposobila servis, a havarije nisu retke. Zato se servis mora obezbediti na dva ili više nezavisnih sistema, tako da ako je jedan od njih onesposobljen, ostali preuzimaju posao, možda sa malo slabijim performansama, ali bez ispadanja. U nekom jednostavnom slučaju mogu, recimo, da se kreiraju dva *e-mail* servera, *mail1.firma.rs* i *mail2.firma.rs*, pa da se svi zahtevi koji stižu na *mail.firma.rs* distribuiraju tako

Sigurnost podataka je jedan od važnih aduta za prelazak u cloud. Gledano iz ugla pojedinačnog korisnika ili manje firme, podaci u nekom OneDrive, Dropbox ili Google Drive skladištu su veoma sigurni

da jedan ide na *mail1*, sledeći na *mail2* i tako u krug. Ako *mail2* nije raspoloživ, sav posao će privremeno obavljati *mail1*.

To lepo zvuči kod servisa koji obrađuju neke konekcije, ali podatke ne možete tek tako držati na dva računara – ubrzo bi informacije bile nekonzistentne. Na *Linux* platformi se u tu svrhu često koristi *Distributed Replicated Block Device* (DRBD) mehanizam koji, na nivou kernela, sinhronizuje podatke smeštene na više servera. Možete to pojednostavljeno zamisliti kao neki RAID, samo što se ne radi o više diskova u jednom kompjuteru, nego o više kompjutera u istom klasteru. Ako se koristi *Windows Server* okruženje, treba proučiti *Windows Server Failover Clustering* mehanizme.

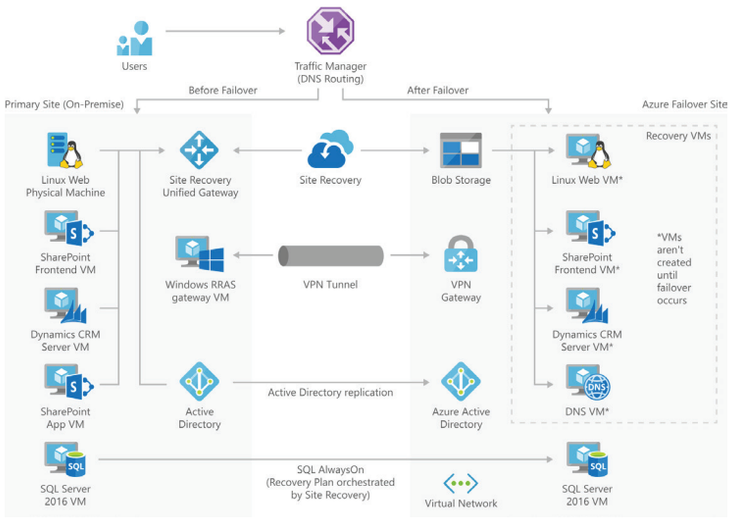
Backup kao servis

Duplirani ili utrostručeni podaci nikako ne znače da je problem *backup*-a rešen. Da, zaštitili smo se od kvara nekog računara, ali ako se *ransomware* zapati na glavnom sistemu, sve te kopije će biti kriptovane. Zato u pozadini treba imati još jedan set servera koji povremeno kopiraju podatke sa produkcionog sistema, ali to neće biti NAS koji samo skladišti podatke, već sistem jednak produkcionom.

Ukoliko osnovni serveri „padnu“, *backup* serveri se mogu odmah proglasiti za glavne servere, ali bez mogućnosti upisa izmena (izmene bi trebalo skladištiti negde drugde), dok se ne shvati kako su glavni serveri kompromitovani i zatim oni vratili u funkciju. U zavisnosti od frekvencije kopiranja podataka, *backup* serveri nemaju baš ažurno stanje svega, što će predstavljati problem, ali će barem sistem brzo biti reaktiviran.

Među procedure za *backup* sistema treba uključiti i redovnu kontrolu ispravnosti napravljenog *backup*-a. Jedini način da budete sigurni da je to što imate relevantna kopija jeste da pokušate vraćanje svega na sistem za testiranje *backup*-a. On treba da testira funkcionalnosti rezultujućeg sistema, i da proveri konzistentnost podataka.

Probni *restore* je dobra prilika da se proceni koliko je vremena potrebno za vraćanje podataka, kako biste imali predstavu o tome koliko će sistem biti nedostupan u slučaju realne havarije. Na osnovu toga možete da napravite koliko-toliko precizan plan za tu potencijalno komplikovanu proceduru.



Šematski prikaz enterprise arhitekture, gde se Azure infrastruktura koristi kao failover sistem na koji obrada prelazi u slučaju kraha produkcionog sistema

Ako se u otpornost sistema uloži više para, moguća su i pouzdanija rešenja u kojima su svi uneseni podaci *read-only* tj. ne mogu se menjati, nego se izmene beleže kao dalje (opet *read-only)* transakcije, pa se do ažurnog stanja dolazi primenom svih transakcija na osnovni podatak. Ako je budžet još veći, *read-only* promene bi se replicirale kroz niz *data* centara. Mnogo zavisi i od prirode podataka, koliko se oni često menjaju i koliko im se često pristupa.

Ne smete imati ni jedan servis koji se izvršava na samo jednom računaru – bilo kakva havarija tog računara bi onesposobila servis, a havarije nisu retke

U oblaku je sigurnije?

Sigurnost podataka je jedan od važnih aduta za prelazak u *cloud*. Gledano iz ugla pojedinačnog korisnika ili manje firme, podaci u nekom *OneDrive, Dropbox* ili *Google Drive* skladištu su veoma sigurni. Treba proveriti šta vaša pretplata podržava, ali ako plaćate bilo šta, sva je prilika da se čuvaju ne samo tekuće datoteke, nego i njihove prethodne verzije, možda i pola godine unazad. Ako *ransomware* šifruje vaše podatke, biće samim tim šifrovani i podaci u *cloud*-u, ali ćete se lako vratiti na prethodnu, ispravnu verziju koja je nedostupna zlonamernom softveru koji se zapatio na vašem računaru.

A ako neko hakuje infrastrukturu koju koriste *Microsoft, Google* ili *Dropbox?* To deluje kao prilično neverovatan događaj, ali zašto biste neograničeno verovali u bilo čiju kompetentnost? Neki korisnici su napravili skriptove koji, recimo, *backup*-uju podatke sa *OneDrive*-a na *Dropbox*, ali nama se najviše sviđa da podatke imamo kod sebe. Ako se koristi bilo koji *sync tool*, kopija (original?) je po prirodi stvari na lokalnom disku, ali povremeno treba praviti i kopiju na hard-disk koji nije stalno uključen, već se bezbedno krije u nekoj fioci ili sefu.

Ako koristite *cloud* za ozbiljnije stvari nego što je skladištenje podataka, dakle ako tamo imate virtuelne servere ili čitavu infrastrukturu, stvari postaju komplikovanije. Ne možete očekivati da će neko rešiti sve vaše probleme, ali vam itekako može pomoći prilikom njihovog rešavanja. Ukoliko koristite *Azure* infrastrukturu, treba da automatizujete konfigurisanje *Azure* resursa *(Infrastructure as Code, IaC)*, što vam daje mogućnost da od razvojnog okruženja po potrebi brzo napravite test okruženje, a od test okruženja produkciono okruženje. Dobar link za početak pretrage bezbednosnih tema je *Azure Disaster Recovery* servis, *azure.microsoft.com/en-us/solutions/backup-and-disaster-recovery/*.

Neki korisnici su napravili skriptove koji, recimo, backup-uju podatke sa OneDrive-a na Dropbox, ali nama se najviše sviđa da podatke imamo kod sebe

Vaši podaci i vaš ICT infrastruktura su sigurni onoliko koliko želite, to jest koliko ste spremni da platite. Račun može da se plaća pre nego što nastupe problemi ili, što je *Garmin* iskusio, kada se katastrofa već desila. U drugom slučaju račun je mnogo veći, ne samo u novcu već i u reputaciji firme, pa i njenom tržišnom uspehu. Najvažnije je učiniti da bezbednost bude proces, a ne niz jednokratnih akcija – ako vas čitanje ovog teksta navede da napravite *backup*, to je svakako dobro, ali ne znači previše. Potrebno je da napravite sistem koji će učiniti da se podaci redovno i automatski čuvaju, a da ispad bilo kog segmenta infrastrukture ne onesposobi čitavu firmu na duže vreme. Posle toga možete da razmišljate o balansu između cene i efikasnosti oporavka od IT katastrofe.

Cloudian hiperskladište za objekte

Simple Storage Service (S3), koji je pokrenuo *Amazon* u okviru AWS-a (*Amazon Web Services*), postao je „de facto“ standard za skladištenje objekata u oblaku. Kompanije i programeri koji implementiraju S3 aplikacije koje se mogu pokretati u lokalnom ili hibridnom (privatnom) oblaku trebalo bi ozbiljno da razmotre *Cloudian HiperStore*® jer već postojeće HTTP S3 aplikacije za klijente rade i čak mogu da koriste isti AWS S3 SDK za pravljenje S3 aplikacija. Dakle, razvoj je, barem za znalce AWS-a, već dobro poznat, a skladištenje svega što je potrebno za rad neke aplikacije, u okviru jednog objekta, donosi nesumnjive prednosti.

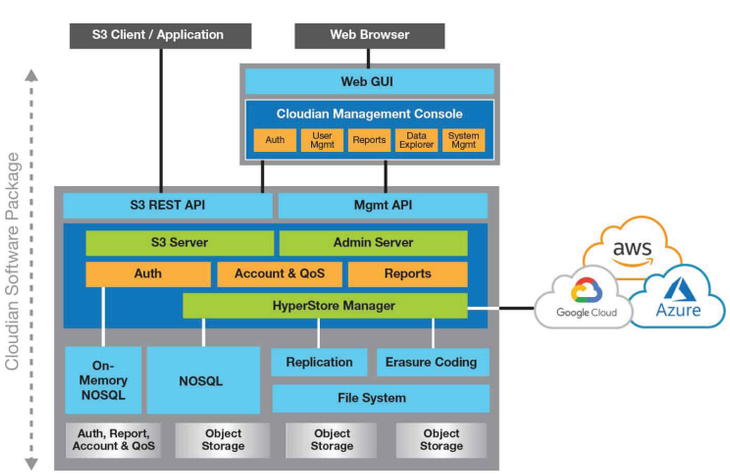
Siguran rad...

Teško je nabrojati sve prednosti koje donosi *Cloudian HyperStore*, ali neke od najznačajnijih su lako alociranje potrebnog storidž prostora, koje se odvija potpuno automatski kroz „katalog servisa“ ili čak *on-demand*, ako to aplikacija zahteva i ako je korisnik dozvolio. Nema nikakvog nepotrebnog čekanja.

Administratori *Cloudian HyperStore* sistema imaju, sa svoje strane, niz pogodnosti za upravljanje sistemom, pa se prava i kvote dodeljuju grupama (*per-group*) ili pojedincima (*per-user*) uz mogući prioritet (favorizovanje) pojedinih grupa i korisnika koji će uvek imati prednost pristupa u slučaju približavanja limitima iznajmljenih resursa.

Cloudian HyperStore može da definiše politiku slojevitosti (*Tiers*) po grupama. Objekti u nekoj grupi mogu se vezati za *Amazon* S3 ili *Glacier*, *Google Cloud Platform*, *Microsoft Azure*, drugi *HyperStore* klaster ili čak bilo koji S3 kompatibilni sistem za skladištenje van mreže, poput trake. *Cloudian HyperStore* može da obuhvati proizvoljan broj nodova u ovim sistemima.

Sigurnost podataka može se kontrolisati na više načina i definisati u zavisnosti od vrednosti podataka. Na snazi su dva ključna metoda osiguranja. *Replication* obezbeđuje postojanje više kopija nekog objekta, po želji na različitim nodovima koje *HyperStore* obuhvata. Još sigurniji sistem zaštite je *Erasure Coding* koji objekte smešta parcijalno – veličinu fragmenata i raspored po nodovima sistema možete da definišete. Redundantnost postoji i ovde, pa objekat ne može da se „izgubi“ čak i ako svi nodovi nisu dostupni.



Da li je podatke bolje čuvati kod sebe ili u nekom cloud servisu? Najbolje je kad imate izbor i međusobnu kompatibilnost koja omogućava čuvanje na oba mesta, pa time i lakši bekap podataka, što će vam omogućiti Cloudian HyperStore

...i na pristupačnom hardveru

Svaki nod *Cloudian HyperStore* sistema zapravo je S3 server koji može da isporuči podatke do bilo kog drugog servera koji je u klasteru. To omogućava veoma lako proširivanje *HyperStore* sistema kroz dodatne *cloud* ili privatne *cloud* servere čak i u različitim *data* centrima. Dodatno, ovakvo povezivanje obezbeđuje i pravu *peer-to-peer* platformu s drastično smanjenim mogućnostima za greške ili pojavu uskih grla.

Poput besprekornog rada, *Cloudian HyperStore* obezbeđuje i vrlo jednostavnu inicijaciju, fleksibilno iznajmljivanje i lako tarifiranje. Primera radi, pri angažovanju prostora do 100 GB, tipična cena angažovanog prostora je oko 0,1 dolar mesečno po gigabajtu.

Sistem automatski vodi statistiku o „potrošnji“ grupa ili pojedinačnih korisnika. Na kraju ugovorenog obračunskog perioda generiše se račun koji, opet, može da bude po grupama ili po pojedinačnim korisnicima, što je automatski i transparentan proces.

Cloudian HyperStore Connect for Files (CHCF) omogućava i standardne fajl servise preko *Cloudian HyperStore* objekta za skladištenje koristeći standardne protokole kao što su NFS, CIFS i FTP. Okruženja zasnovana na datotekama takođe imaju ogromne koristi od bogatih funkcija svojstvenih *Cloudian HyperStore* objektima, kao što su velika sigurnost, izdržljivost, dostupnost, a pogotovo spremanje podataka na više serverskih nodova koji mogu biti veoma udaljeni.

➔ *info@clico.rs*

Inovacije u ponudi donose prednosti vezane za brzinu i ekonomičnost backup-a i oporavka u slučaju katastrofe. Hewlett Packard Enterprise, iako formalno relativno mlada firma, iza sebe ima decenije iskustva u ovoj oblasti...

Marko Herman

Backup i oporavak na HPE način

Gubitak podataka jedan je od najvećih strahova kompanija. Ili bi bar trebalo da bude, a mere za adekvatnu zaštitu su jedan od ne samo informatičkih, već i poslovnih prioriteta! Zašto? Samo pogledajte primer kompanije *Garmin*: sve je počelo 23. jula i prvim izveštajima da je deo *Garmin*-ovih servisa nedostupan – tačnije *Garmin Connect* sajt i mobilna aplikacija namenjeni korisnicima fitnes uređaja. Kasnije istog dana, postale su nedostupne i usluge namenjene korisnicima *Garmin Pilot* i *flyGarmin* aplikacija namenjene avio-industriji. „Pali“ su i kontakt-centri kompanije, a potom je zaustavljena i proizvodnja novih uređaja.

Učite na (tuđim) greškama

Garmin je bio žrtva *ransomware* napada, koji je najverovatnije rešen plaćanjem otkupnine i potonjom dekripcijom svih podataka i oporavkom sistema. Kratkoročni efekat na poslovanje kompanije je zaustavljen, ali dugoročni efekat će se tek osetiti. Koliko potencijalnih korisnika će tri puta razmisliti pre nego što kupi *Garmin*-ov uređaj? Koliki deo tržišta će kompanija izgubiti? Da ne pričamo o reputaciji. Sve to je moglo biti drugačije da su odgovarajuća bezbednosna pravila bila uspostavljena, a svi podaci i sistemi na pravi način *backup*-ovani i čuvani na udaljenoj lokaciji namenjenoj baš ovakvim situacijama – brzom oporavku u trenucima kada je primarni sistem ugrožen!

Brojke su neumoljive. Po IBM-ovom istraživanju, prosečna šteta od ovakvih i sličnih napada je 3,86 miliona dolara. U *Garmin*-ovom slučaju to je najverovatnije 10 miliona direktno za otkupninu, plus svi budući gubici kao posledica. U proseku, čak 39 odsto finansijske štete od napada nastaje više od godinu dana nakon što dođe do neželjene situacije.

Veliki broj kompanija nikad se ne oporavi od ovakvih situacija. To se posebno odnosi na male biznise koji nemaju adekvatnu finansijsku snagu. Čak 20 odsto se zatvori – privremeno ili trajno.

Nova generacija uređaja

Kompanija *Hewlett Packard Enterprise*, iako formalno relativno mlada, iza sebe ima decenije iskustva u domenu IT infrastrukture, *data* centara, *backup* i *disaster recovery* rešenja. Svoje obimno iskustvo i znanje, pretočila je u niz proizvoda i usluga

HPE StoreOnce Catalyst protokol

Situacija s početka teksta ne može da se desi u okruženju koje se štiti na pravi način, a u HPE *StoreOnce* ekosistemu jednu od najbitnijih uloga u tome igra protokol Catalyst. Radi se o protokolu za *backup* koji je kompanija razvila za primenu u *backup* sistemima baziranim na diskovima. Ukratko, HPE *StoreOnce Catalyst* koristi se za čuvanje, replikaciju i arhiviranje podataka tako što korisnici kreiraju *Catalyst* „skladišta“ na *StoreOnce* uređajima ili u *cloud*-u. Ovaj protokol *ransomware* napadači ne umeju da prepoznaju i stoga ne mogu da ga presretnu.

namenjenih kompanijama svih veličina. Na prvom mestu, kao osnova, tu je nova generacija HPE *StoreOnce* fizičkih uređaja za skladištenje i *backup* podataka. Uređaji su projektovani tako da optimalno rade u *cloud* okruženju, a omogućavaju skaliranje u zavisnosti od potreba. Od modela koji će s lakoćom opslužiti male kancelarije, do onih koji će zadovoljiti potrebe najvećih organizacija i provajdera.

HPE *StoreOnce* uređaji omogućavaju jednostavno kreiranje efikasnog i pouzdanog *backup*-a u *cloud* okruženju. Integracija je neprimetna i bez potrebe za dodatnim *gateway* uređajem (bilo fizičkim, bilo virtuelnim). Time se skraćuje vreme, smanjuju troškovi i upotreba mrežnih resursa.

Portfolio ovih uređaja je tako definisan da se lako skalira, u rasponu od modela 3620 koji daje 1,9 PB efektivnog prostora do modela 5650 sa čak 104 PB efektivnog prostora. Ovaj nivo iskorišćenosti omogućen je inteligentnom deduplikacijom podataka koja troškove i potreban prostor smanjuje i do 95 odsto. Uz to, brzina *backup*-a do 288 TB na sat omogućava čuvanje velikih količina podataka u rekordnom roku, kao i vrlo brz oporavak kad se za tim pojavi potreba, tako da vaše poslovanje minimalno trpi.

HPE *StoreOnce* portfolio zasnovan je na najboljoj praksi zaštite podataka koja obuhvata enkripciju rezervnih kopija, redovne provere integriteta, kontrolu pristupa prema ulogama u organizaciji, brz oporavak i visoku dostupnost *storage*-a. Kompleksnost prilikom primene smanjena je objedinjavanjem svih informacija bitnih administratorima, dok korisnici koji svojim aplikacijama sami upravljaju imaju na raspolaganju lak način kontrole zaštite, od *data* centra do *cloud* okruženja.

Uz mogućnost softverski definisane zaštite virtuelnih i *cloud* okruženja, plaćanje po obimu upotrebe i fleksibilno planiranje kapaciteta, HPE *StoreOnce* omogućava kompanijama da zaštite svoju investiciju u sistem za *backup*.

Backup u oblacima

Drugi bitan segment HPE ponude za *backup* predstavlja *Cloud Volumes Backup* – nova usluga namenjena velikim organizacijama, koja pruža jednostavan, efikasan i fleksibilan način čuvanja rezervnih kopija podataka. Ovaj servis može da radi i s tuđim hardverskim rešenjima, ali se sa HPE uređajima jednostavno i savršeno integriše.

HPE Cloud Volumes Backup korisnicima omogućava da u roku od nekoliko minuta povećaju raspoloživ kapacitet, dok automatske *backup* polise eliminišu manuelni rad oko inicijalizacije, podešavanja i upravljanja fizičkom ili virtuelnom infrastrukturom.

Za razliku od konkurencije, HPE *Cloud Volumes Backup* odlikuje se objedinjavanjem *backup*-a u *cloud*-u da bi se izbegla fragmentacija, kao i mogućnošću da se *backup* podaci koriste aktivno za test i developerske potrebe. HPE ne naplaćuje naknadno za oporavak podataka iz *cloud* okruženja, a omogućava da se oporavak uradi na opremu koju kompanija već ima ili u javno *cloud* okruženje.

Primena *Catalyst* protokola znači i da je *backup* nevidljiv za *ransomware*, što obezbeđuje integritet podataka i uspešan oporavak ako do napada dođe. S druge strane, deduplikacija štedi prostor koji zauzima *backup* i ta ušteda može ići i do 20 puta.

HPE *Cloud Volumes Backup* i HPE *StoreOnce* uređaji nove generacije čine vrhunski tandem za očuvanje poslovnog kontinuiteta svake organizacije.

➔ ***hpe.com***

Mali NAS velikog srca

Synology NAS uređaji su moderne storage jedinice za zahtevne pojedince i manje kompanije

Marko Herman

Prethodnih godina testirali smo nekoliko *Synology* NAS uređaja i svaki put smo bili impresionirani. Bilo da je reč o modelu RS815+ namenjenom ugradnji u orman ili o modelu DS1517+ koji je u PC#246 dobio preporuku urednika, naš zaključak je bio da se radi o odličnom rešenju za poslovne storage i *backup* potrebe korisnika.

Danas je pred nama malo drugačiji uređaj – NAS koji cilja pojedinačne korisnike i male firme, a nosi oznaku DS720+ i jedan je od najnovijih modela iz „plus“ serije.

Synology DS720+ ima dva HDD slota koja podržavaju i najnovije diskove kapaciteta 16 TB, kao i dva slota za M.2 SSD koja služe za keširanje podataka radi bržeg pristupa sadržajima. Ugrađen je *Intel Celeron* J4125 procesor radnog takta 2 GHz s *turbo boost* opcijom koja ga ubrzava do 2,7 GHz, što uz 2 GB radne memorije (proširivo do 6 GB) omogućava ovom uređaju da s lakoćom obavi i veoma intenzive zadatke.

U NAS je ugrađen operativni sistem *Disk Station Manager* koji omogućava se DS720+ brzo pripremi za ulogu ličnog storidža i bekap arhive, a uz pomoć pametnog alata *QuickConnect* moći ćete da se na njega povežete preko Interneta i koristite ga kao lični *cloud*.

Bez obzira na to da li uređaj koristite za lične ili poslovne potrebe, odgovoriće na vaše zahteve zahvaljujući dodatnim aplikacijama koje je *Synology* pripremio. To su *Photo Station*, *Video Station* i *Audio Station* alati koji omogućavaju da sadržaj NAS-a koristite i delite. A tu je i *Drive Server* aplikacija koja je namenjena svima koji žele da sa javnog *cloud* okruženja pređu na privatni *cloud*.

Kompletnom sadržaju vašeg storidža možete da pristupite i preko pametnog telefona!

Bezbednost i proširivost

Ako se brinete o zaštiti osetljivih podataka, tu je *Synology* paket *Active Backup for Business* koji omogućava objedinjavanje podataka iz fizičkih i virtuelnih okruženja, kao i brz oporavak fajlova, kompletnih mašina i virtuelnih okruženja kada je to potrebno, bez ikakvog troška za dodatne licence.

Synology DS720+ NAS omogućava i enkripciju foldera, a radi i kao VPN server, tako da vaš pristup na daljinu može biti potpuno bezbedan.

Ukoliko vas postojanje samo dva HDD slota brine, nema razloga za to. NAS se može proširiti uređajem *Synology* DX517 koji ima slotove za još pet diskova, tako da ćete teško ostati bez potrebnog kapaciteta bilo da DS720+ koristite kao kancelarijski storidž ili za čuvanje velike količine multimedijalnog sadržaja (svi znamo kako brzo mogu da narastu lične foto i video arhive).

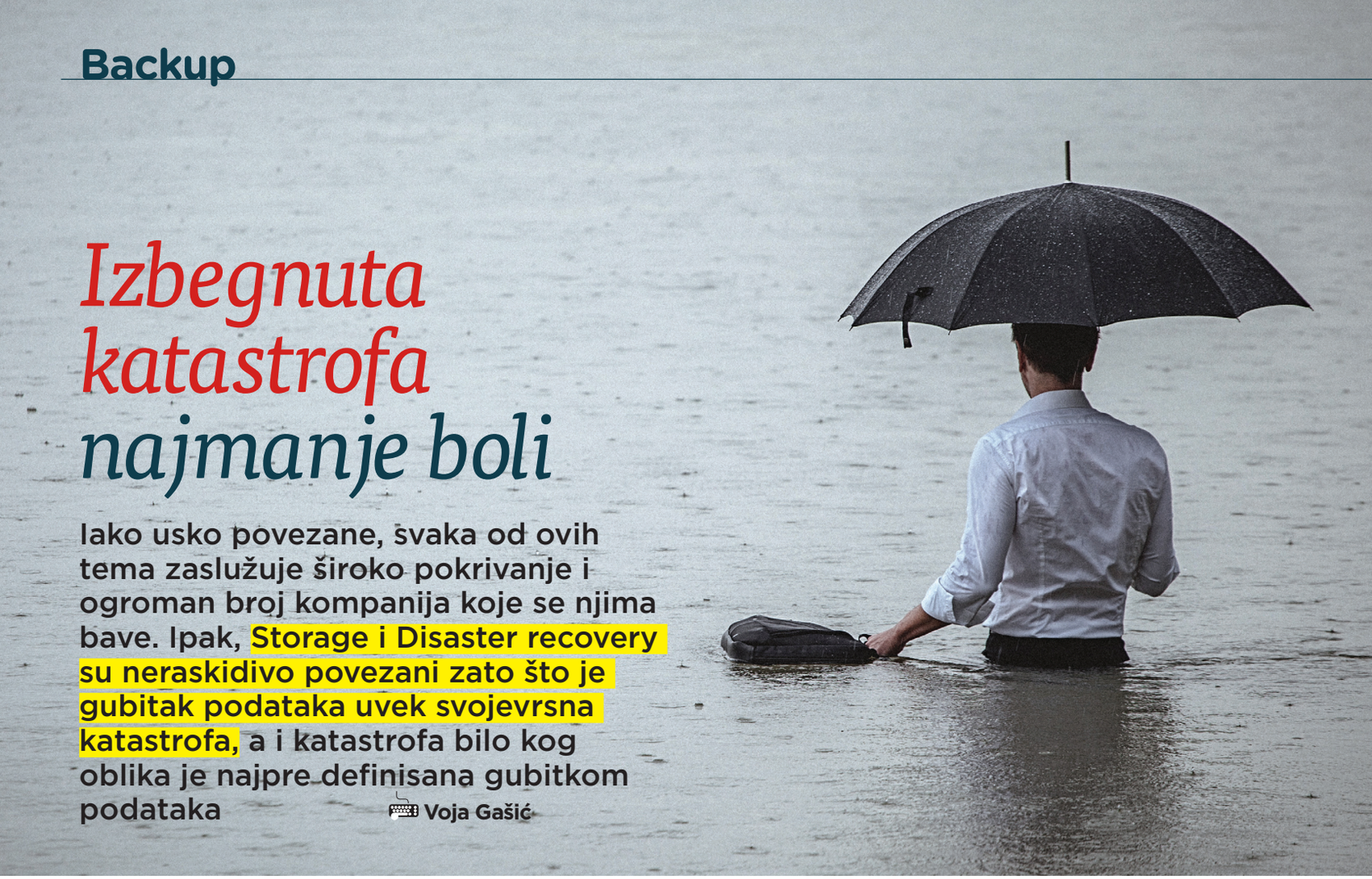
Zahvaljujući inovativnom pristupu i modernom softveru, možemo reći da će ovaj NAS uređaj zadovoljiti i najzahtevnije korisnike.

➔ synology.com

Upoznajte Synology

Kompanija *Synology*, specijalizovana za NAS rešenja, ove godine proslavila je 20. rođendan. Od skromnih početaka na Tajvanu, danas je to globalna kompanija sa šest ogranaka širom sveta, sa stotinama partnera i više od 6.000.000 instalacija! Posvećeni su transformisanju načina na koji organizacije upravljaju svojim podacima u smeru jednostavnosti, bezbednosti i pouzdanosti.

Synology prodaje Tehno Dućan



Izbegnuta katastrofa najmanje boli

Iako usko povezane, svaka od ovih tema zaslužuje široko pokrivanje i ogroman broj kompanija koje se njima bave. Ipak, Storage i Disaster recovery su neraskidivo povezani zato što je gubitak podataka uvek svojevrsna katastrofa, a i katastrofa bilo kog oblika je najpre definisana gubitkom podataka

Voja Gašić

Čak i kada vaša kompanija nema mnogo IT prohteva ili zahteva za čuvanjem dokumentacije, neke osnovne potrebe ostaju. Uredno knjigovodstvo zahteva da se dokumenti (ugovori, računi...) čuvaju, barem neko određeno vreme, a njihova digitalizacija će svakako pomoći – čak i ako ste popularni „direktor @ sam svoj gazda“, elektronska dokumentacija će vam pomoći da savremenije vodite svoj posao.

Ako je sve samo u papirima, može da se desi poplava, požar, da kuče izgricka fasciklu ili registrator s dokumentacijom, a to su sve katastrofe. Možda ne opšte kataklizme, ali svakako katastrofe za vas ako vam neka kontrola zatraži dokumentaciju ili se pojave neki sporni momenti u minulim ili tekućim poslovnim aktivnostima.

Digitalizacija dokumentacije je svakako poželjna opcija, čuvanje ovih digitalnih zapisa na barem dva mesta takođe, a *data retention* vrlo poželjna opcija. *Data retention* zapravo znači beleženje svih koraka i promena u poslovanju, a ne malo je „iskomplikovana“ prisustvom GDPR-a ili zakona o zaštiti ličnih podataka.

Kako vaša kompanija raste i raste broj klijenata, situacija može samo da se pogoršava. Zato pažljivo, uz proveru zakonskih akata, a ako je potrebno i uz konsultacije sa stručnim licima ili timovima, treba pristupiti planiranju toga šta se i gde beleži, gde se čuva, kome je dostupno i u kom vremenskom periodu.

Da, morate omogućiti da se bitni podaci i dokumentacija čuvaju, da se osigura njihovo čuvanje na više mesta, ali da ne nestanu u nekoj prirodnoj (ili neprirodnoj) katastrofi ili, još gore, da osetljivi ili nečiji lični podaci ne dospeju ne neke pogrešne ruke. Sve su to katastrofe na koje morate da računate, ma koliko je mala verovatnoća da se zaista dese. I sve se tiču vaših podataka ili nečijih tuđih, a vama poverenih podataka.

Pet razloga zašto vam je potreban plan oporavka od katastrofe

Svet je nepredvidiv, a neka katastrofa može da nastupi u bilo kom trenutku. Kupujete osiguranje da biste finansijski zaštitili svoje poslovanje od gubitaka, ali osiguranje ne može da zameni dragocene podatke, ključne aplikacije koje čine vaše poslovanje uspešnim i već postojeće korisnike od (privremenog) gubitka kontakta s vama. Da biste zaštitili te stavke, nije dovoljno uplatiti osiguranje. Morate da planirate unapred, kreirajući plan za vraćanje podataka ako se izgube. Razmotrite narednih pet situacija koje bi mogle pogoditi vaše poslovanje i krenite u planiranje.

Prirodne katastrofe

Majka priroda može biti okrutna. Oluje, požari i poplave sve mogu da nanesu nepopravljivu štetu vašoj kompaniji. Bez uspostavljanja jasnog plana za oporavak od katastrofe, možda će vam biti izuzetno teško da nastavite sa radom, što će dovesti u pitanje budućnost vaše kompanije. Oko 80 odsto kompanija koje se zatvore na period duži od 5 dana nikada se više ne otvore, pa je brzo ponovno postavljanje proizvodnje (delatnosti) na noge ključno u slučajevima prirodnih katastrofa.

Kvar hardvera

Bilo da dođe do prenapona struje ili ako vam hardver zakaže iz nekog drugog razloga, to može odneti sa sobom sve vaše podatke. Iako možete da preduzmete korake za zaštitu vašeg hardvera sistemima za hlađenje, zaštitnicima od prenapona i drugom tehnologijom. Od presudne je važnosti da redovno pravite rezervne kopije podataka. Korišćenje storidža zasnovanog na *cloud*-u ili van redovne lokacije može doneti dodatnu zaštitu, jer je malo verovatno da će obe lokacije biti istovremeno pretrpeti neku ozbiljniju katastrofu, pogotovo ako su lokacije na razumnom fizičkom rasto-

janju. Vaš plan za oporavak od katastrofe treba da sadrži ove korake, da biste sprečili potencijalni gubitak podataka.

Uvek postoji opcija da poslovanje i podatke (ili neki deo) prepustite nekom drugom iznajmljujući resurse u data centru, ali nekada se i ozbiljnim data centrima dešavaju havarije.

Ljudske greške

Niko nije savršen, a to na žalost uključuje i vas i vaše zaposlene. Ako zaboravite da sačuvate izmene u dokumentu, slučajno obrišete važan dokumenat, pa i slučajno uključivanje/isključivanje pogrešnog prekidača, može da dovede do značajnog gubitka za vašu kompaniju. Programi obuke mogu da pomognu u smanjenju grešaka, ali jedini način da se vaše poslovanje zaista zaštiti od gubitka podataka zbog ljudske greške je redovno pravljenje rezervnih kopija podataka.

Cyber zločini i zločinci

Na žalost, *cyber* zločini su u stalnom porastu i većina preduzeća u nekom trenutku biva pogođena. Napad virusa ili *ransomware*-a (naš slučaj) mogao bi zaustavi vaše poslovanje i uzrokuje velike gubitke profita. U težem slučaju, mogli biste duže da ostanete taoci zlonamernih hakera. Zato vaš plan za oporavak od katastrofe treba da sadrži korake za oporavak od pokušaja hakovanja, čuvajući vaše podatke bezbednim i dostupnim na više mesta.

Služba za korisnike

Na kraju, potreban vam je plan za oporavak od katastrofe da biste svojim klijentima pružili uslugu koju očekuju od vas. Ako se vaše preduzeće mora zaustaviti ili ako dođe do dužeg prekida usluga, sva je prilika da ćete izgubiti veći broj vrednih kupaca u odnosu na konkurenciju. Što brže možete povratiti svoju operativnost, vaši klijenti biće srećniji i nećete im dati mnogo vremena za premišljanje i promenu dobavljača.

Nijedan posao, pogotovo oni poslovi koji se više oslanjaju na IT podršku, nije imun na rizik od gubitka pristupa podacima i aplikacijama. Plan oporavka od katastrofe može vam pomoći da se osigura da gubitak ostane mali i privremeni problem, uz brzo obnavljanje vašeg poslovanja. Ova kontrolna lista može vam pomoći da započnete u kreiranju plana koji može zaštititi vaše poslovanje od raznih potencijalnih katastrofa.

Backup & Restore

U svim katastrofičnim scenarijima je bekap podataka i aplikacija, te njihov brzi povratak i oporavak od ključnog značaja za brzo vraćanje funkcionalnosti. Bez obzira na to za koji sistem se odlučite kad je u pitanju skladištenje vaših rezervnih podataka (*backup*), ponovićemo staru krilaticu da se bekap pravi u nadi da nikada neće zatrebati.

Ipak, čak i bezazlene greške nekada mogu prouzrokovati gubitak podataka, pa bekap ipak mora da bude dobro isplaniran. Tu najpre mislimo na činjenicu da bekap mora da bude dovoljno čest jer ćete u protivnom restaurirati sistem u neko davno prošlo vreme i, u najboljem slučaju, moraćete naknadno da unesete sve podatke koji nedostaju – ako se uopšte setite koji su to podaci i ako oni budu dostupni.

S druge strane, beleženje cele slike sistema (*system image*) zajedno sa svim pripadajućim podacima može da bude vrlo zahtevno – i vremenski i kad su u pitanju resursi. Planiranje ispravne frekvencije bekapa sistema i podataka je vrlo značajna stavka, ali je veoma dobro da se raspitate o mogućim rešenjima koja omogućavaju i frekventnije, inkrementalno upisivanje rezervne kopije podataka. Pravilnim planiranjem, smanjićete zahteve za velikim storidžom, a da to ne ide na štetu brzine oporavka u slučaju da je restauracija (*restore*) sistema ili podataka neophodna.

„Sitne stavke“ od značaja

Zanimljivo je da naši partneri pišu i o drugim aspektima sprečavanja gubitka podataka ili funkcionalnosti, pa svakako treba istaći i značaj dobre klimatizacije i pravilnog (i rezervnog) napajanja sistema. Uvek postoji opcija da ove brige (ili neki njihov deo) prepustite nekom drugom iznajmljujući resurse u *data* centru, ali nekada se i ozbiljnim *data* centrima dešavaju havarije – jednoj od njih bili smo svedoci krajem avgusta.

Drugo rešenje je da se upustite u avanturu sopstvenog data centra. Neka od rešenja nude *Vertiv* i *Vesimpex* u obliku potpuno funkcionalnih i po svim pravilima izvedenih mikro data centara. Za poslove koji uključuju ozbiljno angažovanje ICT resursa, to je i preporučena varijanta jer *Edge data centar* je *cloud*, ali vaš *cloud* i pod vašom je kontrolom.

Najvažnije je da na vreme izračunate koliko bi vašu kompaniju koštao gubitak podataka ili gubitak funkcionalnosti. Shodno tome, isplaniraćete sredstva, vreme i dodatne aktivnosti da do katastrofe ne dođe. Ili bar da se verovatnoća svede na minimum.

6 koraka do disaster recovery plana

Bez obzira na veličinu, broj zaposlenih, industriju i tržište na kojem posluju – savremene kompanije postaju sve bolje u prepoznavanju prednosti ulaganja u razvitak svojih IT infrastruktura. Prema istraživanju kompanije Dell, čak 71 odsto preduzeća razume ulogu tehnologije u kontekstu sticanja i održavanja konkurentne pozicije na tržištu

Pored toga, ukoliko odluče da jedan deo budžeta posvete digitalnom unapređenju poslovanja, preduzetnici mogu da očekuju smanjenje troškova na duge staze. Poslovni procesi se optimizuju i delom automatizuju, što pospešuje i ukupan nivo produktivnosti.

Zvuči sjajno, zar ne?

Ipak, postoji i manje primamljiva strana priče, a tiče se ranjivosti IT infrastruktura i važnosti dobro definisanog plana oporavka u slučaju katastrofe, odnosno *disaster recovery* plana.

Šta je disaster recovery plan i zašto vam je potreban

Odgovorno poslovanje podrazumeva prevenciju kao strateški pristup, pogotovo kada je reč o čuvanju kompanijskih podataka od važnosti.

Uprkos ulaganjima u visoku zaštitu kompanijskih podataka, nijedna IT infrastruktura nije 100 odsto bezbednosno zaštićena od potencijalnih katastrofa. Uobičajene prakse poput upotrebe naprednih antivirus softvera, šifriranja informacija, uvođenja strogih pravila privatnosti, ograničavanja pristupa malom broju osoba od poverenja – ipak ne garantuju da se ništa loše ne može desiti, mada minimiziraju mogućnost narušavanja bezbednosti.

Nažalost, katastrofe se dešavaju. One mogu biti izazvane:

- Ljudskom greškom ili svesnim, zlonamernim delovanjem grupe ili pojedinca
- Iznenadnim kvarom na hardveru
- Krađom IT opreme
- Uspešnim hakerskim napadom
- Bilo kakvim spoljnim uticajima (poput požara i poplava, ekstremnih vremenskih uslova, havarija) koji su doveli do nestanka struje ili fizičkog oštećenja infrastrukture u sklopu kolateralne štete

Prilično je jasno da katastrofu teško možete predvideti.

Ali možete da mislite unapred i napravite detaljan plan oporavka (tj. *disaster recovery* plan), kako biste se u najkraćem mogućem roku i uz minimalne gubitke vratili u normalan ritam poslovanja.

Dobar plan podrazumeva sveobuhvatnu dokumentaciju koja jasno definiše protokol i procedure, te obezbeđuje kontinuitet u poslovanju i brzo sanira štetu.

Kako doći do njega?

Manje primamljiva strana IT priče tiče se ranjivosti IT infrastrukture i postojanja dobro definisanog disaster recovery plana, odnosno oporavka u slučaju katastrofe

KORAK #1:

Izlistajte sva IT sredstva koja posedujete i procenite rizik

Logičan početak za izradu *disaster recovery* plana podrazumeva popis i analizu važnih podataka koji su ključni za poslovanje, kao i popis hardvera i sistema koje vaše preduzeće poseduje i kojima upravlja. Na taj način možete jasno definisati elemente vašeg poslovnog IT okruženja i odrediti za šta je sve odgovoran IT menadžment.

Uobičajena IT sredstva čine:

- Serveri
- Različite vrste aplikacija i programa
- Podaci (npr. kontakt podaci poslovnih partnera, poverljivi podaci mušterija i korisnika)
- Mrežni uređaji i pristupne tačke sistemu
- Konkretna oprema i uređaji za skladištenje podataka i slično.

Nakon popisa, sledi procena rizika. Za svaki od elemenata koji ste uvrstili u svoju tabelu navedite potencijalne pretnje i rizike. Vaš stručni IT tim ili koordinator za bezbednost trebalo bi da proceni nivo rizika za svaku stavku.

KORAK #2:

Organizujte elemente po faktoru kritičnosti

Glavna uloga *disaster recovery* plana je da vam omogući da u slučaju katastrofe, sistematično i hladne glave povratite svoju kompaniju na noge, uz najmanji mogući zastoj u poslovanju. Zbog toga je važno da napravite stručnu klasifikaciju svih elemenata unutar tabele i poređate ih po faktoru kritičnosti, to jest definišite koji su elementi od najveće važnosti za celokupno poslovanje firme.

U ovom procesu trebalo bi da učestvuju koordinatori iz različitih sektora kompanije kako bi se prilikom prioritetizacije uzela u obzir celokupna slika poslovanja, a ne subjektivni utisak pojedinaca.

KORAK #3:

Sastavite budžet i odaberite prave saveznike

Sasvim očekivano, nakon procene rizika, sledi procena troškova za saniranje potencijalne štete. Formiranje budžeta u okviru *disaster recovery* plana iziskuje vreme, ali je nužno radi što efektnijeg rukovođenja kompanijom u kriznoj situaciji.

Jedna od korisnih caka za formiranje budžeta jeste da prvo popišete najvrednije stvari (velike stavke poput održavanja softvera i hardvera, plata zaposlenih, prostora gde se skladište podaci i sl.) i da zatim unosite manje troškove.

Sve zavisi od rizika kojem ste izloženi. U svakom slučaju, cifre ćete najlakše definisati oslanjajući se na svoju prethodnu fiskalnu godinu, tj. uobičajene prihode i troškove.

U današnje vreme, *cloud* usluge dobijaju sve značajnije mesto u kontekstu prevencije i osmišljavanja efektnog i pristupačnog *disaster recovery* plana. Uz *cloud*, podaci se čuvaju *offsite* odakle se bezbedno mogu preuzeti u slučaju katastrofe. Stepen zaštite IT sistema je visok, a ne postoje nikakvi skriveni niti uzaludni troškovi: kompanije plaćaju samo ono što zaista i potroše, što čini ulaganje u *cloud* mudrom poslovnom odlukom.

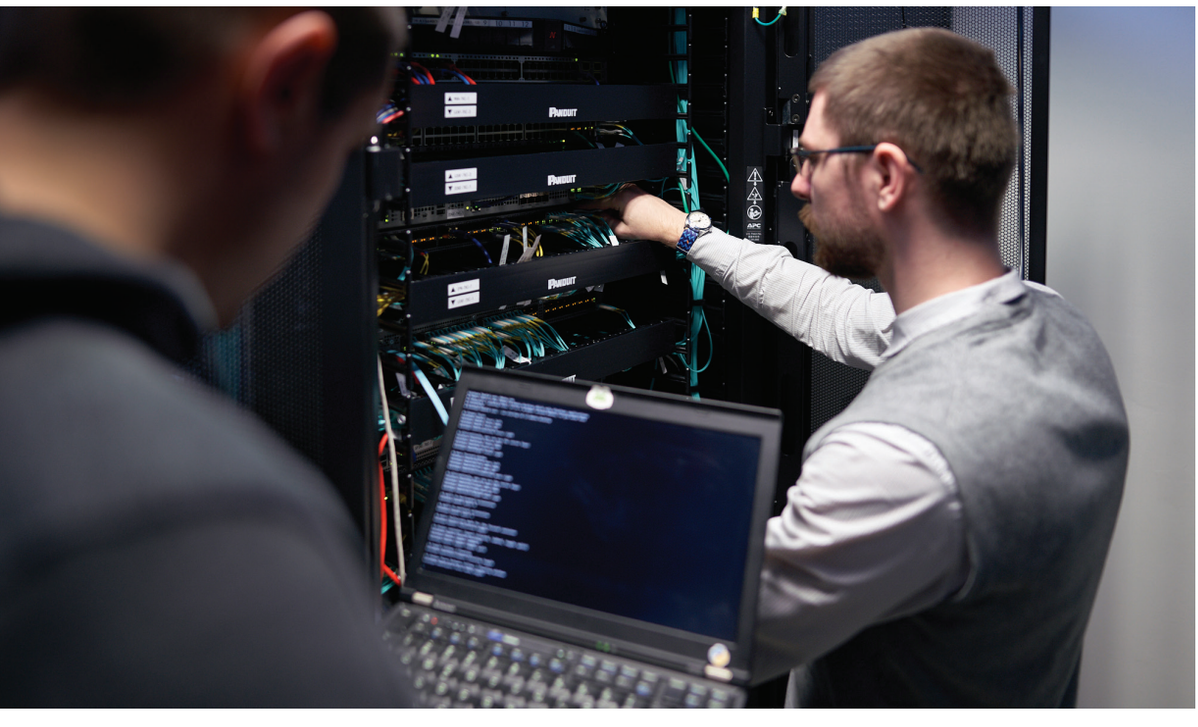
KORAK #4:

Definišite period i tačku oporavka

Prilikom izrade *disaster recovery* plana, neophodno je definisati period oporavka (*recovery time objective*) i tačku oporavka (*recovery point objective*).

Period oporavka podrazumeva unapred definisan maksimalan period za sprovođenje *disaster recovery* plana. Naravno, ovde je u pitanju odokativna ocena, ali se ipak ne sme svesti na nagađanje. U proces definisanja perioda oporavka moraju biti uključeni članovi višeg menadžmenta koji bi trebalo da daju krajnje odobrenje.

Tačka oporavka odnosi se na prihvatljivu količinu podataka koju kompanija može da izgubi, a da to ozbiljno ne naruši ritam poslovanja. Od ove definisane vrednosti zavisi učestalost *backup*-a kako bi se svi ključni podaci sačuvali. Ukoliko kompanija pretrpi ozbiljan pad sistema, tačka oporavka omogućuje vraćanje podataka sačuvanih u sklopu najskorijeg *backup*-a. Njome se definiše i starost datoteka koje se moraju povratiti.



Pokušajte da kontinuirano testirate vaš plan kroz obuku zaposlenih, slično kao s protivpožarnim vežbama. Ne samo da ćete kroz treninge dostići visok nivo uigranosti, već i usavršiti plan oporavka.

KORAK #5:

Definišite strateške aktivnosti i dodelite odgovornosti

Vratimo se na vašu *Excel Sheet* tabelu. Do sada ste izlistali sve elemente, sortirali ih po faktoru kritičnosti, definisali sve pretnje, nivo verovatnoće za svaki od rizika, kao i moguće nivoe štete.

Sada je vreme da definišete tačan protokol, tj. strateške aktivnosti, i to:

- Strategiju odgovora ili reagovanja (*response strategy)*
- Strategiju oporavka (*recover strategy)*

Za obe strategije neophodno je da definišete jasne korake kako biste u slučaju katastrofe staloženo odreagovali.

Pogledajmo to na pojednostavljenom primeru podataka o iznosima obaveza kompanije, elementa koji će se sasvim sigurno naći u vašoj tabeli.

Kako su u pitanju ključni podaci koji se tiču finansija, oni se negde moraju skladištiti, te ćemo kao potencijalni rizik staviti pad servera.

Kao strategiju odgovora možemo staviti *backup* servera, a koraci bi uključivali sledeće:

1. Potvrditi da je server pao
2. Potvrditi da su podaci bezbedno sačuvani na *backup*-u
3. Prebaciti podatke na privremeni server

Kao strategiju oporavka možemo staviti popravku ili zamenu primarnog servera koji je u nekom trenutku otkazao, a koraci bi uključivali sledeće:

1. Utvrditi razlog pada servera
2. Instalirati novi server
3. Testirati novi server
4. Prebaciti podatke na novi server

Pisanje operativnih procedura možda nije najzabavnija stvar na svetu, ali je ključna u sklopu formulisanja *disaster recovery* plana. Katastrofe ostavljaju za sobom visokostresnu atmosferu i često su pod naborjem panike. Imati jasno uputstvo koje vas, korak po korak, podseća šta bi trebalo da radite – od neprocenjive je vrednosti.

KORAK #6:

Dokumentujte, testirajte i evaluirajte svoj plan

Poslednji korak podrazumeva jasno dokumentovanje *disaster recovery* plana, kao i njegovo testiranje. Potom sledi evaluacija i eventualne prepravke onoga što ste zabeležili.

Pokušajte da kontinuirano testirate vaš plan kroz obuku zaposlenih, slično kao s protivpožarnim vežbama. Ne samo da ćete kroz radionice i treninge dostići odličan nivo uigranosti već ćete, takođe, identifikovati manjkavosti vašeg plana i stoga ga usavršiti. Uz to, vaše poslovanje će se s vremenom menjati, kao i IT sredstva koja koristite i kojima upravljate, te *disaster recovery* plan nužno mora da prati sve promene.

➔ ***mainstream.rs***

Primer iz prakse
AIK banka

Ljubiša Radivojević, CEO Mainstream

Kompanija *Mainstream* ima bogat portfolio klijenata koji uključuje ugledne kompanije iz različitih industrija, kao što su AIK banka, NIS, Sberbanka, *KupujemProdajem*, *Gomex*, *Limundo*, Televizija PRVA, *Gigatron*, B92, *Tehnomanija* i mnogi drugi. Jedan od zahtevnijih projekata bilo je unapređenje i optimizacija disaster recovery rešenja za AIK Banku.

Ljubiša Radivojević, CEO *Mainstream*-a, ističe da je ovo bio izazovan projekat, ali da su zahvaljujući dobroj i prisnoj saradnji sa AIK bankom rezultati bili odlični: „*Disaster recovery* podrazumeva rešenje koje obezbeđuje kontinuitet poslovanja u slučaju nepredviđenih okolnosti (npr. iznenadni kvar na hardveru, ljudska greška, hakerski napad ili fizičko oštećenje infrastrukture). AIK banka, kao jedna od vodećih u Srbiji, uživa veliko poverenje svojih klijenata, te bi svaki minut nedostupnosti sistema predstavljao rizik za realizaciju prihoda i izgrađenu reputaciju. Iz IT ugla, *Mainstream* je odigrao važnu ulogu u procesu spajanja AIK banke i Alpha banke (kasnije preimenovane u Jubanku) – budući da smo izveli integraciju IT sistema dveju banaka i uspeli da unapredimo infrastrukturu zarad najvišeg stepena bezbednosti. Pored toga, ispoštovali smo postojeće tehnologije i topologije i uspeli da smanjimo IT troškove za više od 40 odsto.“

BIZIT

SEDMA BIZIT KONFERENCIJA

D!BUSINESS
2020

4. i 5. novembar 2020.
Klub poslanika, Tolstojeva 2, Beograd
Ili tamo gde ste vi

PRIJAVITE SE I OSTVARITE
POPUST ZA RANU PRIJAVU

WWW.BIZIT.RS