Varnostna kopija, **kot se šika**

Rezervno kopiranje je eno izmed redkih področij, kjer bi lahko rekli, da je pretirana ali paranoična skrb dobrodošla. Žal pa še vedno prevečkrat velja, da uporabniki stvari uredimo šele takrat, ko smo vsaj enkrat izgubili dragocene podatke. Najceneje se je torej učiti na napakah drugih.

Matic Zupančič

Kaj lahko gre narobe?

Vse. Vaše podjetje lahko propade, proizvodnja obstoji ali pa si na glavo nakopljete zajetno tožbo.

Poglejmo samo primer katastrofalne odpovedi strežnika, ki mu je prisostvoval avtor tehle vrstic. Na kratko bomo povzeli: v nekem podjetju se je ponoči pokvaril strežnik in obenem se je, kako prikladno, sesulo tudi diskovno polje. Imeli so varnostno kopiranje, ki pa, glej ga zlomka, ravno takrat ni delovalo. Povedano drugače: varnostne kopije niso imeli že dalj časa, kajti kabel, ki naj bi povezoval tračno enoto s strežnikom, je obvisel nekje v zraku v prenatrpani strežniški omari. Na diskih so bile recepture za njihove slastne izdelke in brez njih je proizvodnja stala. Če bi bilo varnostno kopiranje urejeno, kot se šika, bi proizvodnja stala morda eno izmeno, tako je pa ves teden, dokler laboratorij za reševanje podatkov ni opravil svoje čarovnije.

Kaj je varnostna kopija?

Pozabite na ročno premikanje datotek z diska na zunanji disk. To ni varnostna kopija. To je kopiranje, ki deluje kakšen teden, dva, v najboljšem do prvega dopusta delavca, ki bi moral vsak dan ali teden ročno premikati datoteke. Jasno je, da se po dopustu na take stvari pozabi.

Efektivna izdelava varnostne kopije je avtomatiziran proces, ki mora čim bolj izključiti človeški dejavnik. Če gre kaj narobe, mora sistem skrbnika na e-pošto ali še bolje z esemesom obvestiti o nenarejeni varnostni kopiji, da lahko sistemski administrator nemudoma ukrepa.

Dobra rešitev varnostnega kopiranja mora biti sposobna povrniti stanje podatkov na neko določeno časovno točko (denimo včeraj zvečer ali še natančneje 15. 5. 2020).

Primer: če je podjetje prizadel kripto virus danes zjutraj ob 9.22 in če vemo, da delamo varnostne kopije ob 3. uri ponoči, mora znati program za varnostne kopije iz vseh podatkov sestaviti stanje podatkov, kot je bilo ob izdelavi kopije, torej ob 3.00 tisti dan, pred napadom virusa.

Če se gremo ročno kopiranje, lahko hitro naredimo napake, namenski programi za varnostne kopije pa vse skupaj opravijo z lahkoto.

Morda najpomembnejša postavka v definiciji učinkovite varnostne kopije je tudi preverjanje, ali se iz rezervno kopiranih podatkov dejansko da podatke tudi restavrirati. Ne nazadnje je ravno to smisel vsega skupaj, kajne? Bolj malo smo naredili, če vemo, da se ponoči nekaj nekam kopira, nismo pa stoodstotno prepričani, da lahko s temi podatki tudi rešimo poslovanje podjetja, če se zgodi katastrofa.

Kaj NI varnostna kopija?

Mnogokrat slišimo: »Na strežniku imam štiri diske, torej je za varnostne kopije poskrbljeno.« Hmm, ne. Ne bo držalo. To je le redundanca diskovja za primer

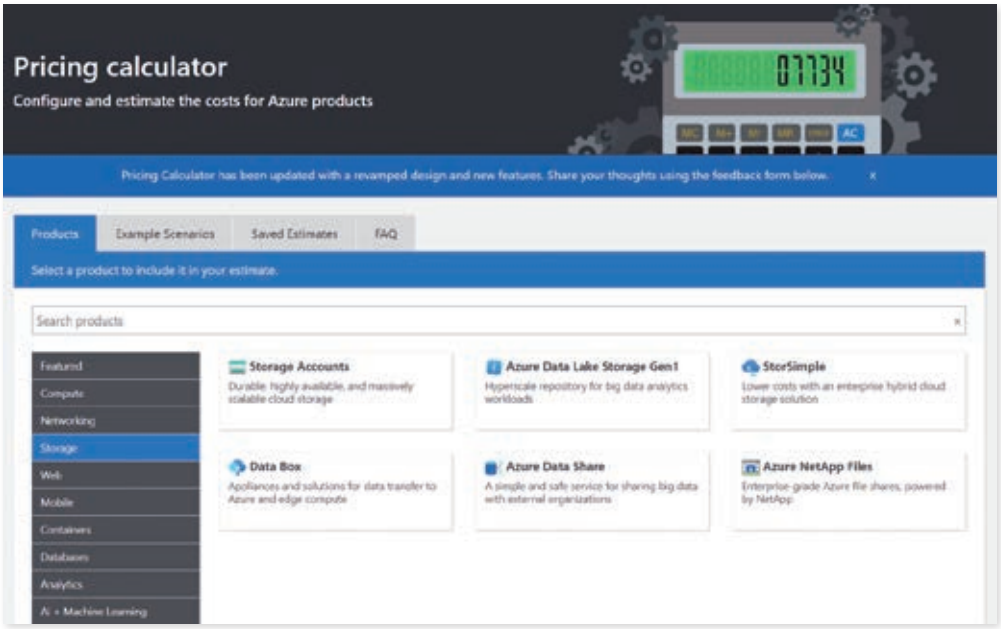
V nekem podjetju se je ponoči pokvaril strežnik in obenem se je, kako prikladno, sesulo tudi diskovno polje. Imeli so varnostno kopiranje, ki pa, glej ga zlomka, ravno takrat ni delovalo.

odpovedi strojne opreme. Diska. Vsak podatek na disku ima tudi kontrolni seštevek in zaradi tega diskovno polje lahko deluje tudi, ko se eden od diskov pokvari. Ko ga zamenjamo, se manjkajoči podatki dobesedno izračunajo in zapišejo nazaj na nov disk.

Največkrat so diskovna polja z redundanco označena s stopnjo RAID. Pri RAID 1 gre, denimo, za zrcaljenje diskov. RAID 1 z dvema diskoma lahko »preživi« okvaro kateregakoli izmed njiju in sistem bo še vedno deloval. Seveda je treba okvarjeni disk takoj zamenjati.

V podjetjih so pogostejši sistemi RAID 5, RAID 6 in RAID 10, ki imajo različne stopnje redundance, pri kateri se lahko pokvari tudi večje število diskov naenkrat. Glavni dodatni razločevalni dejavnik pri odločitvi pa so hitrostne karakteristike, saj stopnja RAID in število diskov v polju določata tudi hitrost pisanja v polje in branje iz njega. Ampak to je že zgodba za ločen članek. Vrnimo se k rezervnim kopijam.

Ob napadu kripto virusa nas



△ **Kalkulator stroškov je uporaben, ko želite približno oceniti stroške najema prostora v Azure.**

Praksa!

Zavedati se morate, da vsaka varnost nekaj stane. Brez nekaj finančnega vložka vsekakor ne bo šlo. Če ne drugega, potrebujete zadovoljivo količino prostora na diskovju. Najbolje boste storili, če si omislite kar omrežni disk (NAS), na katerega boste delali lokalne rezervne kopije. In nato si nabavite še enega, da boste lahko delali kopijo prvega. Pa smo šele pri drugi kopiji. Za tretjo kopijo lahko seveda kupite še en NAS in ga postavite na neko tretjo lokacijo z dobro povezljivostjo. Lahko pa uporabite oblak.

Pa pojdimo kar h konkretni postavitvi za potrebe malega podjetja, ki smo jo videli že večkrat tudi v praksi in je zato preizkušena.

Potrebna strojna oprema: dva omrežna diska Synology DS-418, napolnjena vsak s po štirimi diski 3 TB, kar na vsakem izmed omrežnih diskov da 9 TB prostora za podatke.

Pa začnimo

Na omrežnem disku naredite mapo, v katero boste odlagali rezervne kopije. Nato naredite še posebnega uporabnika, ki ima dostop izključno in samo do mape, ki ste jo ravnokar naredili. Pri vsem skupaj pazite, da uporabnik v sistemu nima nobenih drugih pravic, razen branja in pisanja v to mapo. Administratorskemu računu obvezno vzemite pravice do branja in pisanja v to mapo. Podatki vam bodo hvaležni.

Druga zelo pomembna stvar, na katero morate paziti pri konfiguraciji, je, da do omrežnega mesta za varnostna kopija ne dostopate iz Windows Explorerja (Raziskovalca), kajti v tem primeru se vam utegne zgoditi, da se bodo dostopni podatki samodejno shranili v upravitelju poverilnic (*Credential Manager*). In to je zadnja stvar, ki jo želite. Zakaj? Ker bo kripto virus te poverilnice izkoristil za nemoteno pisanje po mapi rezervnih kopij in jih bo zašifriral.

Naslednji korak sta namestitev Veeam Agenta na računalnik in njegova konfiguracija. Ko vpisujete podatke za dostop do mape za varnostno kopijo, vpišete uporabnika, ki ste ga ustvarili na omrežnem disku.

Odločiti se boste tudi morali, ali boste delali rezervno kopijo posameznih map, posameznih diskov ali pa ustvarili kar kopijo celotnega računalnika. O prednostih zadnjega smo se razpisali zgoraj, in če imate dovolj prostora na diskovju, je to najbolj priporočljiva možnost.

Koliko obsežno časovno razdobje boste hranili v arhivu, je v prvi meri odvisno predvsem od tega, kako veliko je diskovno polje oziroma koliko naprav boste rezervno kopirali.

Vam v korist pa gre dejstvo, da so varnostne kopije optimizirane ter stisnjene in zato en teden rezervnih kopij ne pomeni seštevka sedmih kopij vseh podatkov, marveč precej manj.

Druga kopija

Tako, eno kopijo od treh ste si že zagotovili in lahko se lotite druge. V drug prostor znotraj podjetja, še bolje pa na tretjo lokacijo, kjer imate dostop do službenega omrežja, namestite drug omrežni disk Synology. Med programsko opremo, ki je na voljo v operacijskem sistemu omrežnega diska Synology, boste našli Hyper Backup Vault, ki je potreben, da bo lahko en omrežni disk zapisoval na drugega.

Na prvem omrežnem disku pa boste pognali Hyper Backup. V tej aplikaciji boste ustvarili opravilo, ki bo dnevno kopiralo podatke s prvega omrežnega diska na drugega. In stvar je načelno opravljena. Z nekaj kliki, torej.

Tretja kopija

Če bi se držali priporočil kot pijanec plota, bi vam morali svetovati, da celotno kopijo podatkov shranite še nekam v oblak. A ob veliki količini podatkov, ki se dnevno spreminjajo, lahko postane shranjevanje v oblak časovno in ne nazadnje tudi finančno precej požrešno.

Morda boste torej morali ubrati drugačen, kompromisen pristop. Če je skupna količina podatkov v rezervnih kopijah manjša od 8 TB, je najhitrejša rešitev nakup zunanjega diska USB. Priklopite ga na enega izmed omrežnih diskov in v aplikaciji Hyper Backup na omrežnem disku ustvarite novo opravilo, ki podatke shrani še na ta ravnokar dodani nosilec.

Če želite še malenkostno zakomplicirati postavitev, boste nabavili dva taka zunanja diska in ju boste izmenično tedensko menjali, prostega pa zaupali v varstvo svoji tašči. Slaba stran

število diskov v strežniku ali diskovem polju prav v ničemer ne zaščiti, saj ne omogoča restavriranja podatkov na določeno točko v preteklosti. V primeru napada kripto virusa gre namreč za logično poškodbo podatkov, diski so ob vsem skupaj povsem zdravi in normalno delujejo.

Tudi sinhronizacija ni varnostna kopija

Uporabnike mnogokrat zbega tudi razlika med rezervnim kopiranjem in sinhronizacijo. V načinu sinhronizacije delujejo najrazličnejše storitve tipa Dropbox ali OneDrive. A če imate svoj OneDrive sinhroniziran s službenim računalnikom, to še ne pomeni, da so podatki tudi »varnostno kopirani«. Zakaj? Predstavljajte si, da se vaš računalnik okuži z izsiljevalskim virusom. Ta bo zašifriral lokalne podatke in program za sinhronizacijo bo vse te spremembe nemudoma poskusil prenesti v oblak. V takih primerih si s sinhronizacijo lahko zataknete zanko okrog vratu, namesto da bi vas rešila. Potrebujete torej rešitev varnostnega kopiranja, ki bo sposobna povrniti podatke iz neke časovne točke, preden so se okvarili ali jih je nekdo izbrisal oziroma spreminjal.

△ Pravilo rezervnega kopiranja. 3 kopije podatkov. 2 različna medija. 1 kopija zunaj.

Mnogokrat slišimo: »Na strežniku imam štiri diske, torej je za varnostne kopije poskrbljeno.« Hmm, ne. Ne bo držalo.

Postulat 3 – 2 – 1

Lahko se prepiramo o tem, katera rešitev za varnostne kopije je najprimernejša, kateri diski so bolj vzdržljivi in kateri ponudnik shrambe v oblaku je boljši, a o osnovnem aksiomu varnostnega kopiranja ni debate. Vedno velja 3 – 2 – 1. Imeti moramo najmanj tri kopije podatkov, na najmanj dveh različnih nosilcih in najmanj ena kopija mora biti na drugi lokaciji.

Vzemimo za primer pametnega fotografa, ki se drži pravil dobrih praks. Ima tri popolne kopije svojih podatkov, eno kopijo na omrežnem disku, drugo takega polavtomatskega načina je, seveda, spet človeški dejavnik, ki po naših izkušnjah vedno zataji.

Ko pa je cilj tretja kopija prav v oblaku, hkrati pa želite količino prenesenih podatkov vseeno minimalizirati, boste posegli po orodjih, ki so dosegljiva v strežniških operacijskih sistemih, ali po orodjih tretjih proizvajalcev.

In spet ste pred dilemo …

H kateremu ponudniku odložiti podatke?

Priporočamo pragmatičen pristop. Ni vse v ceni. Veliko pomeni tudi ugled podjetja. Če se ozremo po pokrajini ponudnikov shranjevanja podatkov v oblaku, tako zasledimo podjetja, ki so že uveljavljena in imajo tudi zrele produkte, ki večinoma ne zatajijo.

Izpostavili bi predvsem dva. Microsoft Azure in Amazon Glacier. Prvi je priporočljiv za uporabo takrat, kot želite rezervno kopirati podatke z Windows strežnikov, saj ti že v osnovi podpirajo zapisovanja v Azure že od različice 2016 naprej, seveda pa ima podporo zanj tudi marsikateri omrežni disk, ne le omenjeni Synology.

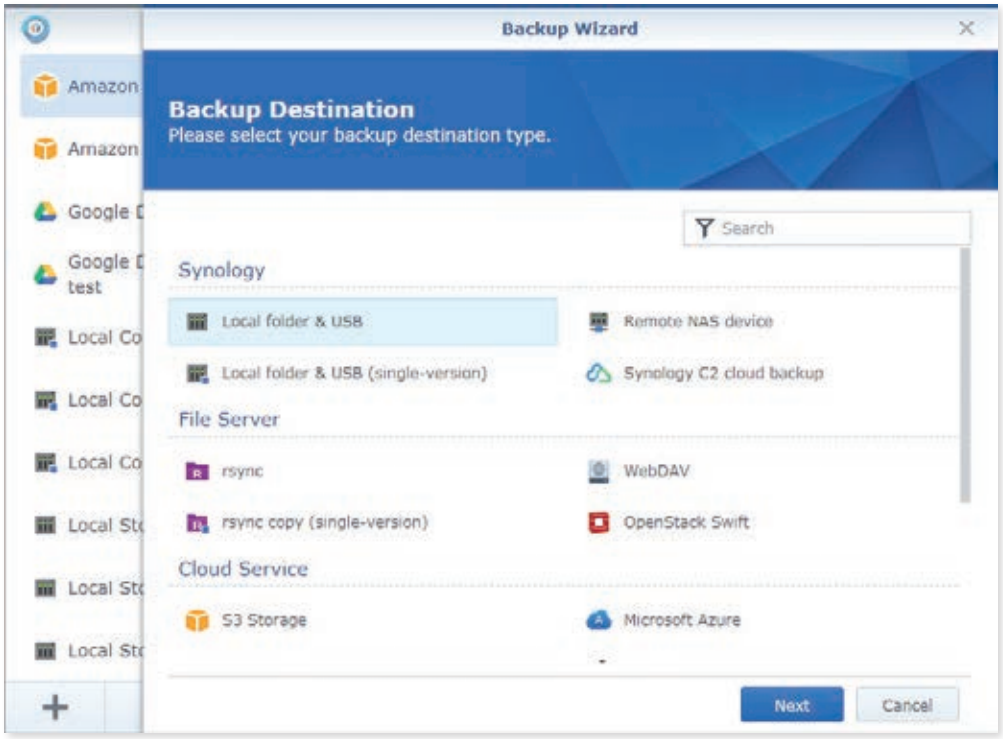
Amazon Glacier in Microsoft Azure sta zanimiva predvsem zaradi svoje cenovne ugodnosti, a je zaradi načina obračunavanja ravno pri njiju težje oceniti, kakšni bodo dejanski stroški takšne hrambe. Medtem kot drugi večji ponudniki ponudijo fiksno ceno za gigabajt ali količinsko omejene pakete s fiksno ceno, je pri omenjenih dveh ponudnikih nekaj specifike. Cena na gigabajt je res nizka in tja lahko spravite toliko podatkov, kolikor vam srce poželi ali denarnica dovoli, a obračunane bodo tudi operacije PUT in GET pa tudi količina podatkov, prenesenih iz oblaka k vam.

Povedano drugače: potiskanje podatkov v Azure in Glacier je brezplačno, plačevali boste neko smešno nizko ceno na gigabajt shrambe, ko pa boste te podatke zahtevali nazaj, restavriranje ne bo več tako poceni, saj se pretok podatkov iz oblaka k uporabniku obračuna posebej in ne stane malo.

A če ste si tak način rezervnega kopiranja izbrali po pameti in imate urejeni vsaj še dve kopiji podatkov, je varnostna kopija v oblaku tako in tako le *last resort* kopija, ki jo boste uporabili samo v skrajni sili, v kateri še pregovorni hudič žre muhe in boste večji strošek restavriranja lahko upravičili.

Še eno stvar je treba omeniti. V Azuru lahko izberete možnost dostopa do podatkov *archive*, kar je cenovno najugodnejše, a hkrati to pomeni, da boste, če bi želeli te podatke restavrirati, nanje čakali tudi do osem ur. Shranjeni bodo namreč na trakove, ki so še vedno v uporabi v velikih data centrih. Podobna časovna zakasnitev velja tudi pri Amazon Glacierju.

Opisana rešitev:
Strojna oprema:
2 × Synology DS-418.
Cena: 2 × 374 EUR + DDV.
8 × WD RED 3 TB.
Cena: 8 × 88 EUR + DDV.
Cena skupaj:
1.452 EUR + DDV.
Programska oprema:
Veeam Backup & Replication Community Edition (do 10 virtualnih strežnikov).
Cena: Brezplačno.



◁ **Omrežni diski Synology imajo enostaven uporabniški vmesnik za konfiguracijo rezervnega kopiranja - vse uredite v aplikaciji Hyper backup.**

Vedno velja 3 – 2 – 1. Imeti moramo najmanj tri kopije podatkov, na najmanj dveh različnih nosilcih in najmanj ena kopija mora biti na drugi lokaciji.

na zunanjem disku (v bistvu dva zunanja diska menjuje enkrat tedensko), tretja kopija pa gre v eno izmed oblačnih storitev (denimo Amazon S3 ali Microsoft Azure). V njegovem primeru so tri (pogojno štiri) kopije, trije nosilci (omrežni disk, zunanji disk, oblak) in dve kopiji zunaj podjetja. Ena zunanja je tista v oblaku, druga zunanja pa je na zunanjem disku, ki kroži in ga nato nese v hrambo svoji tašči.

Mit: Dovolj je imeti varnostno kopijo v oblaku

Večkrat zasledimo razmišljanja poslovodstva in tudi sistemskih administratorjev, da je za podjetje dovolj varno, če ima podatke rezervno kopirane le v oblaku. Res je, da je to še vedno bolje kot biti brez rezervnih kopij, ampak v tem primeru ne gre toliko za varnost pred izgubo podatkov kot za vprašanje nemotenega poslovanja.

Lokalne povezave v podjetju so danes običajno vsaj hitrosti 1 Gb/s, vedno pogosteje tudi 10 Gb/s. Če vzamemo povezavo z internetom 100 Mb/s, je tako potrebnih vsaj 21 ur, da iz oblaka k sebi prenesemo 1 TB podatkov. V lokalnem omrežju se taka količina podatkov prenese v najslabšem primeru v dobrih dveh urah.

Prav zaradi časovne komponente je lokalna kopija podatkov izjemnega pomena.

So podatki v oblaku tudi primerno varovani?

Ker danes večinoma vsi uporabljamo storitve v oblaku (Gmail, Dropbox, OneDrive …), je povsem na mestu vprašanje, ali moramo glede varnostnega kopiranja teh podatkov še karkoli postoriti. Priporočamo, da nikakor na slepo ne zaupate temu, da bodo mega korporacije poskrbele za varnostne kopije vaših podatkov.

Ugibamo, ne da bi se poglobili v pravniško solato splošnih pogojev poslovanja prej omenjenih ponudnikov, a bi si upali dati roko v ogenj, da so jih pravniki dobro oprali vsakršne odškodninske odgovornosti, ki bi izvirala iz izgube podatkov.

Kar lahko storite, je, da redno in avtomatizirano varnostno kopirate podatke v oblaku na omrežni disk ali zunanji USB-disk.

Kaj kopirati? Sliko računalnika ali le uporabne podatke?

Rezervno lahko kopirate tudi le dejanske mape z datotekami, pomembnimi za poslovanje, ki vsebujejo, denimo, dokumente, tehnično dokumentacijo, podatkovne zbirke, računovodske aplikacije in podobno.

S stališča uporabnosti pa je precej bolj zanimiva možnost, da se odločite za rezervno kopiranje celotnega virtualnega ali fizičnega strežnika oziroma računalnika. Programska oprema za varnostne kopije v tem primeru naredi kopijo celotnega sistema, vključno z datotekami operacijskega sistema in zagonskih sektorjev diska, ki omogočajo zagon stroja.

Taka varnostna kopija je zelo zanimiva iz dveh razlogov. Prvič, naredite lahko tako imenovani *bare metal restore* oziroma restavriranje na drugo strojno opremo. Primer: v računovodstvu se pokvari računalnik, ki je za poslovanje podjetja zelo pomemben, saj se z njega opravlja vsa komunikacija z državo in bankami. Ker imate celotno sliko računalnika, lahko mirno kupite nov računalnik in nanj opravite restavriranje okvarjenega računalnika. Računovodkinja bo v nekaj urah spet operativna, vključno z vsemi certifikati in podpisnimi komponentami, ki jih sistemski administratorji sovražimo nameščati.

Drugi razlog za tak način rezervnega kopiranja pa bo najbolj všeč računalnikarjem. Arhiviranje celotnih strežnikov in računalnikov namreč omogoča bliskovito kreiranje testnega okolja, ki je identično produkcijskemu. Uporabna vrednost tega se pokaže, ko je treba testirati nadgradnjo poslovne ali sistemske programske opreme. Seveda pa moramo poudariti, da mora takšno izdelavo testnega okolja podpirati tudi programska oprema za varnostne kopije.

Varnostna kopija Microsoft 365 in G Suite

Se podatkom v oblaku sploh lahko kaj zgodi? Mnogokrat naletimo na mit o tem, da so ponudniki elektronske pošte tako zanesljivi, da teh podatkov pa res ni treba rezervno kopirati. Ne smemo pozabiti, da je oblak dejansko le velikanski kup strežnikov in diskov, zato moramo ohraniti isto mero paranoje, kot jo imamo pri podatkih na lastnem strežniku.

In tako si boste želeli imeti tudi podatke iz Microsofta 365 (nekoč Office 365) ali G Suita varno spravljene nekje drugje v oblaku ali pa pri sebi lokalno.

Ker že tako in tako imate omrežne diske, ki ste jih uporabili v prejšnjih opisanih korakih, lahko uporabite aplikacije, ki so vam na voljo na njih.

Pri Synologyju sta tako najbolj uporabni aplikaciji Active Backup for G Suite in Active Backup for Office 365. Z njima boste k sebi prenesli vsebino celotnih organizacij v oblaku, v primeru Officea 365 tudi datoteke v OneDrivu ter Sharepoint portalu. ◀