

Zaščita najpomembnejšega premoženja organizacij z varnostnim kopiranjem podatkov

Marko Praprotnik, vodja oddelka za upravljanje, nadzor in varnost informacijskih sistemov.

Objavljeno v Varnostni forum, april 2006

Planiranje in izvajanje varnostnega kopiranja podatkov je kompleksni proces, ki se ga je potrebno lotiti načrtno in sistematično. Velikokrat se pomembnosti tovrstnega početja ne zavedamo, saj podatkov iz varnostnih kopij ne potrebujemo vse dokler se z njimi ne zgodi kaj kritičnega. Sam proces varnostnega kopiranja podatkov se pogosto zamenjuje s procesom arhiviranja podatkov, čeprav med njima obstaja pomembna razlika. V primeru varnostnega kopiranja podatkov (angl. Backup) le-te ščitimo pred spremembami, pretvorbami, brisanjem ali koruptiranjem, medtem ko gre v primeru arhiviranja podatkov za dolgoročno shranjevanje podatkov, ki se v poslovnih procesih nič več ne spreminjajo (angl. Records). Arhivirani podatki se ponavadi shranijo na naprave, ki ne dopuščajo sprememb in brisanja (angl. Write Once Read Many), kar zahtevajo tudi nekateri zakonski predpisi in standardi.

Organizacije dandanes potrebujejo orodja za celovito upravljanje s podatki, ki obvladujejo obe navedeni funkciji in veliko več. Pojavljajo se dodatne zahteve po arhiviranju podatkov skladno z zakonskimi predpisi in standardi, transparentnem premikanju zastarelih podatkov med različnimi pomnilniškimi podsistemi, izdelavi analiz izkoriščenosti pomnilniških kapacitet in upravljanju pomnilniških podsistemov. Istočasno ne smemo zanemariti osnovnih zahtev, kot so centralizirano upravljanje in nadzorovanje, enostavna uporaba, visoka varnost shranjenih podatkov, zanesljivost, skalabilnost in nizki stroški lastništva.

Izbira programske opreme, izvajalca, implementacija, podpora ter izbira ustreznega vzdrževanja je ključna za uspešnost projekta in zanesljivo delovanje. Prvi pogoj za uspeh je podrobno poznavanje informacijskega okolja in priprava na izbor programske ter strojne opreme. Natančen popis in informacije o operacijskih sistemih, podatkovnih zbirkah, lastno in nelastno razvitih aplikacijah, količinah podatkov, dnevnih spremembah, neaktivnih podatkih, prenosnih poteh, časovnih okvirih in organizacijskih predpisih so zelo pomemben del planiranja. Le s pomočjo kvalitetnih in popolnih vhodnih podatkov lahko kvalitetno določimo varnostno politiko.

Za pripravo varnostne politike je ključnega pomena poznavanje konceptov izdelovanja varnostnih kopij in rešitev, ki to možnost nudijo. Pomemben del varnostne politike so načini izdelovanja varnostnih kopij podatkov, število hranjenih verzij, časovna okna za shranjevanje in restavriranje podatkov, načini prenosa podatkov, iznosi varnostnih kopij, načrti za okrevanje sistemov in operativna ter varnostna navodila.

Obstaja več različnih načinov izdelovanja varnostnih kopij, ki se razlikujejo glede na ciljni sistem in proizvajalca programske opreme za varnostno kopiranje. Izbira načina varnostnega kopiranja je odvisna predvsem od zahtev organizacije glede

neprekinjenega poslovanja in časovnih oken za shranjevanje in restavriranje podatkov. Prvi izziv je shranjevanje ter restavriranje podatkov operacijskih sistemov. Postopke za to lahko poenostavimo in časovno skrajšamo s posebnimi programskimi moduli za izdelavo posnetkov stanj. Ti nam v primeru kritične napake povrnejo operacijski sistem hitro in brez potrebne prisotnosti usposobljenih upraviteljev. In kar je tudi pomembno, restavriranje operacijskih sistemov v takih primerih ni omejeno na identično strojno opremo. Varnostno kopiranje podatkov datotečnih sistemov lahko izvajamo na različne načine. Neskončno kopiranje (angl. Continuous Data Protection) nam omogoča varovanje podatkov v realnem času. To pomeni, da se takoj po spremembi dokumenta v ozadju že izvede varnostna kopija. Ideja te rešitve izhaja iz prepričanja, da varnostno kopiranje enkrat dnevno preprosto ne zadostuje. Na določenih dokumentih se spremembe lahko dogajajo zelo pogosto, cilj pa je, da se spremembe zaznajo takoj ter se istočasno tudi takoj ustrezno zavarujejo. Aplikacije (lastno in nelastno razvite), podatkovni strežniki in poštni sistemi so naslednji zelo pomembni nosilci podatkov. Varnostno kopiranje teh podatkov brez prekinitve delovanja je ponavadi ključno za vse organizacije. Zelo pomemben del je tudi možnost restavriranja podatkov v točno določen čas (angl. Point in Time) in restavriranje posameznih objektov (angl. Single Object Restore), pa naj si gre za posamezni objekt iz relacijske zbirke ali pošto iz uporabnikovega poštnega predala. Posebni načini varnostnega kopiranja omogočajo, da se izvorni sistem pri izdelavi varnostnih kopij podatkov ne obremenjuje. To je mogoče z uporabo naprednih funkcij preslikave podatkov na pomnilniških podsistemih, ki jih lahko učinkovito uporabimo tudi pri varnostnem kopiranju. Tudi varnostno kopiranje podatkov mobilnih in distribuiranih uporabnikov postaja vse pomembnejše. Njihovi podatki se zaradi vse večjega obsega mobilnega poslovanja in zaradi pogostega neupoštevanja internih organizacijskih pravil še vedno nahajajo na lokalnih pomnilnikih, kjer so podvrženi okvaram, zlorabam in krajam.

Naslednji korak je izbira prenosnih poti in pomnilnikov, kamor se bodo podatki varnostno kopirali. Katere prenosne poti bomo uporabili, je odvisno od količine podatkov in časovnih oken za shranjevanje ter restavriranje podatkov. Podatke lahko prenašamo preko WAN, LAN ali SAN omrežij. Tračne knjižnice s tračnimi mediji so najbolj razširjen način shranjevanja podatkov, ki so rezultat varnostnega kopiranja podatkov. Le-te dosegajo visoke hitrosti in kapacitete. Ker gre za naprave z zaporednim dostopom do podatkov in mehanskimi komponentami, se hitro pokažejo tudi njihove slabosti. Te opazimo pri hitrostih shranjevanja in restavriranja podatkov (predvsem v obliki majhnih datotek ali objektov) ter zanesljivosti robotike, pogonov in medijev. Zaradi tega za primarno varnostno kopijo velikokrat uporabimo tehnologijo, ki nam omogoča naključni dostop do podatkov in bazira na diskovni tehnologiji. Priporoča se, da se primarne varnostne kopije ne iznašajo in so vedno na voljo za primer restavriranja podatkov. Za primer kritične napake je smiselno izdelovati kopije shranjenih podatkov, ki se iznašajo ali samodejno izdelujejo na oddaljeno lokacijo.

Ker varnostne kopije potrebujemo predvsem v neugodnih situacijah, je testiranje integritete le-teh bistvenega pomena. Načrti za okrevanje so pomemben del načrta za neprekinjeno poslovanje organizacij. Načrt za okrevanje natančno določa vse postopke in aktivnosti, ki jih je potrebno v kritičnih situacijah izvesti. Za primer varnostnega kopiranja podatkov ti načrti natančno določajo vse postopke in aktivnosti, ki jih je potrebno izvesti za vzpostavitev okvarjenega sistema. Načrti nastajajo tako, da se iz varnostnih kopij v testnem okolju poizkuša vzpostaviti sistem, pri katerem se vse aktivnosti natančno beležijo. Redno testiranje, popravljanje in dopolnjevanje je ključnega pomena za verodostojnost načrtov za

okrevanje. Samo na tak način lahko odkrijemo morebitne nepravilnosti pri varnostnem kopiranju, spoznamo pasti in posebnosti posameznih aplikacij ter natančno določimo čas, ki ga potrebujemo za vzpostavitev prvotnega stanja.