Kontinuitet rada poslovnog sustava i automatski oporavak sustava u slučaju incidenta u zdravstvenom prostoru

Claudio Škarecki[1], Vjeran Perinović[2], Dražen Pomper[3*], Sara Pomper[4]

[1]*KBC Zagreb, Zagreb, Hrvatska*
[2] *Opća županijska bolnica Požega, Odjel za medicinsku informatiku, Požega, Hrvatska*
[3]*Opća bolnica Varaždin, Odjel za zdravstvenu informatiku, Varaždin, Hrvatska*
[4]*Student treće godine Fakulteta organizacije i informatike Sveučilišta u Zagrebu, Varaždin, Hrvatska*

**e-pošta: drazen.pomper@obv.hr*

Djelatnici u zdravstvenim ustanovama, suočavaju se s ogromnom odgovornošću kada se radi o digitalnim informacijama iz poslovnog svijeta zdravstvenog sustava. Moraju se poštivati svi zakoni i pravilnici kao i direktive, štititi privatnost pacijenata i nadasve osigurati da klinički podaci budu kontinuirano dostupni čak i u slučaju zastoja ili katastrofe. Kako bi se podržala i osigurala kvalitetna njega i skrb o pacijentima, poštujući standarde i težeći ispunjavanju poslovnih ciljeva, mora se stvoriti kontinuirana održivost sustava bazirana na IT platformi. O tome se danas brinu dobro educirani informatičari.

Elementarne nepogode, iskustvo rata iz naše bliske povijesti te ostali čimbenici koji mogu utjecati na zastoj u poslovanju realna su prijetnja i konstantna opasnost na odvijanje svakodnevnih poslovnih funkcija baziranih na IT tehnologijama. Danas je IT bazična domena za sve ostale djelatnosti, one koriste IT kao osnovni pogon za distribuciju poslovnih informacija.

Danas su *cloud* usluge sazrele i kao takve postale održiva opcija za sigurnosno kopiranje podataka zdravstvenih sustava izvan lokalnih prostora, tako da se poslovanje može prebaciti u podatkovni centar i nazad bez zastoja u poslovnim procesima. Postoji sigurnost u radu i *OPEX* model određivanja cijena kojima se štede proračunska sredstva. Osim spremanja podataka, može se imati i kompletne sustave na rezervnoj lokaciji koja se u slučaju potrebe može aktivirati.

Ključne riječi: dostupnost IT sustava; kontinuitet poslovanja; automatizirani oporavak IT sustava; zaštita podataka; antivirusna strategija; IT sigurnost; računalni virusi; poslovanje u oblaku; uredba o zaštiti osobnih podataka; kibernetička sigurnost

Popis kratica i pojmova korištenih u tekstu:

Backup – sigurnosna pohrana podataka

BUaaS – sigurnosna pohrana podataka kao servis

BC - Business continuity – kontinuirani nastavak poslovanja

BYOD - korištenje osobnih uređaja u poslovne svrhe

CAPEX - kapitalni izdaci

Cloud – poslovanje preseljeno u oblak, potpuno ili parcijalno

Data storage - sustav za pohranu podataka

DR - Disaster recovery – potpuni oporavak IT sustava

GDPR - Opća uredba o zaštiti osobnih podataka

HL7 - komunikacijska norma

IaaS - infrastruktura kao servis

IT – informacijska tehnologija

NAS - mrežni sustav za pohranu podataka

OPEX - operativni izdatak

Restore – proces vraćanja podataka iz sigurnosne kopije podataka

RPO - Recovery Point Objective - točka oporavka je vrijeme koje je potrebno da se infrastruktura vrati u radno stanje nakon ponovnog podizanja.

RTO - Recovery Time Objective - vrijeme oporavka je period koji je potreban za ponovnu uspostavu infrastrukture nakon katastrofičnog događaja, tj. vrijeme potrebno za ponovno uspostavljanje sustava.

SOC - sigurnosni operativni centar

Tier - nivoi ili slojevi kod backup-a

Uvod

Projekcija održivosti kontinuiteta poslovanja i procesa potrebnih za oporavak u slučaju raspada IT rješenja spada u domenu redovnih poslova i zadataka informatičara. Pretpostavka je dobra preventiva, dobro posložen informatički sustav, redovno održavan i dograđivan. Nemoguće je predvidjeti sve tehnološke i organizacijske slabosti IT sustava u zdravstvu, zato su planiranje i prevencija osnovni postulati u radu dobrog informatičkog tima. Optimalno posložena IT platforma zahtijeva velika ulaganja u znanje informatičara. Na prvi pogled ulaganje u znanje je skupo, ali neznanje može imati katastrofalne posljedice na poslovanje u zdravstvenom okruženju. Neophodno je da zdravstvene ustanove naprave procjenu rizika svih segmenata poslovanja. U kontinuitetu se za IT područje treba utvrditi poslovni plan, BC (engl. business continuity), zajedno sa planom za postupanje u izvanrednim situacijama, DR (engl. disaster recovery) koji se međusobno dopunjuju.

Da bi sve radilo kako treba, mora se poraditi na svim segmentima razvoja svjesnosti mogućih problema i rizika te prema njima planirati oporavak u slučaju incidenta. Samo višeslojno sigurnosno rješenje daje mir i stabilnost poslovnom medicinskom sustavu podržanom IT tehnologijom. Prelazak u "oblak" dobar je izbor i sve je više parametara da ta strategija dobije dužnu pozornost.

U zdravstvenom sustavu zdravstveni djelatnici stvaraju velike količine podataka o aktualnim zdravstvenim slučajevima, pretežno u multimedijskoj formi. Bazom podataka kroz transakcijski model u načelu se arhivira sadržaj svih poslovnih događaja u tekstualnom formatu, dok se većina suvremene digitalizirane dijagnostike pojavljuje u formatu slike i filma te konverzije zvučnog zapisa. Podaci su nastali kao posljedica znanja i radnog napora medicinske struke u strukturiranom obliku, što je osnovni uvjet za uspješnu digitalnu transformaciju podataka u informaciju (1).

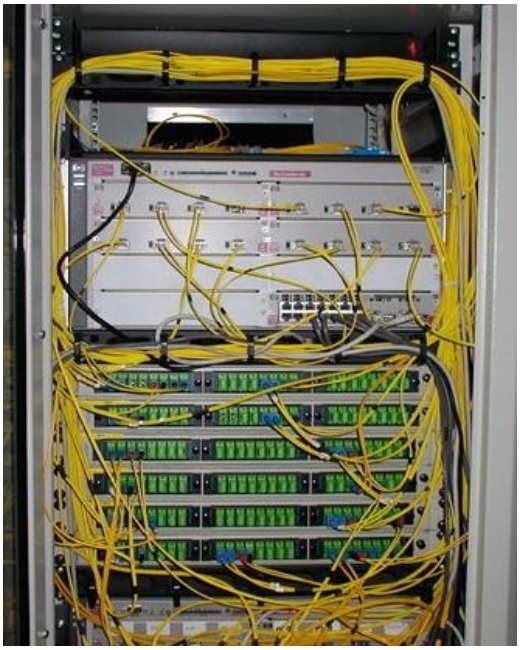
Slika 1. Transformacija poslovanja u digitalnom svijetu, eruptivne aktivnosti uvijek su prisutne

Obradom podataka ustanove dobivaju važne medicinske informacije. U digitalnom svijetu zadaća je informatičara da poslovni sustav održavaju sigurnim i stabilnim. Informatika je dodana vrijednost medicinskoj struci jer čuva ugled zdravstva i daje povjerenje u zdravstveni sustav. Osobni podaci po zakonu pripadaju u posebnu kategoriju povjerljivih podataka. Sistemski inženjeri specijalizirani za sigurnost u virtualnom prostoru drže maliciozne aktivnosti ispred vrata zdravstvenog informatičkog sustava. Znanje uloženo u prevenciju zaštite sustava, održavanje stabilnosti i dostupnost pristupa informaciji zdravorazumska je i zakonska obveza informatičara u zdravstvenom prostoru.

Složena poslovna rješenja treba pratiti sofisticirana informatičko-komunikacijska platforma. IT sektor jedna je od najbrže rastućih inovativnih tehnologija u svijetu. Suština upotrebe moderne informatičke i komunikacijske tehnologije je stvaranje ergonomski optimalnog radnog okruženja. Koncepcija dobre informatike je složiti poslovne uvjete i procese svakodnevnog operativnog posla na najbolji mogući način. Ako je primarni cilj dobivanje više vremena za obradu medicinskog slučaja, jednostavan i brz dohvat informacija, u pozadini moraju biti integrirana kompleksna informatička znanja. Cilj je omogućiti medicinskoj struci optimalno zatvaranje svih procesa u medicinskom slučaju upotrebom IT platforme. Tehnologija mora donijeti komparativnu prednost s kompetencijama za ugled i povjerenje u zdravstveni sustav. Kvalitetna programska rješenja i kontinuirana dostupnost podataka logičan su paket usluga koji se dnevno isporučuje korisnicima sustava. Zdravstveno osoblje više nego ikada koristi i oslanja se na znanje i vještine informatičke struke.

Velika je uloga Odjela za informatiku koji ima kompleksnu internu sistematizaciju posla, ali i ima vrlo dinamičnu strukturu znanja zbog eksponencijalnog rasta razvoja novih rješenja iz IT sektora. Takvo radno okruženje zahtijeva iznimna znanja i vještine, konstantnu edukaciju i

brigu o radu informatičkog sustava koji čine tehnologija, programska rješenja i ljudi. I zakon dedicirano govori o postojanju iznimno tehnički složenih informatičkih sustava u zdravstvenom sustavu, što nalaže ekstremnu brigu i deklarira veliku odgovornost struke koja se brine za rad sustava. Zakon kaže da su medicinski podaci iznimno osjetljivi i kao takvi zahtijevaju dodatni operativni posao, posebnu zaštitu forme i sadržaja, a sve integrirano u pojam informacijska sigurnost. Iskustvo nalaže da se ulaganje u informatičku preventivu višestruko isplati. Rad sustava bez zastoja i incidenata bilo koje vrste, logična je potreba. Informatički se sustav mora staviti u poziciju podrške procesa u zdravstvenoj ustanovi. Sve je digitalizirano, integrirano, u formi interoperabilnosti, pa je logično da tako sofisticiranim sustavima s važnim podacima upravljaju kompetentni informatičari. Broj informatičara mora biti dostatan, a znanja treba permanentno ažurirati. Posao odjela informatike je jasan: održati stabilnost i dostupnost informatičkog sustava. Informatičari su odgovorni za formu sustava: skalabilnost, održivost, integraciju. Za ta područja treba imati iskustvo i znanje, polivalentnu vještinu koja jamči kompetenciju, opstanak sustava i ugled zdravstvene ustanove.



Slika 2. Preklopnici i optička mrežna tehnologija

U održavanje informatičkog sustava uključeni su zanavljanje mehanike i elektronike sustava, poslužitelji, skladišta podataka, radne stanice, mrežna aktivna oprema te oprema za neprekidno napajanje. Kvalitetno vođenje evidencije o informatičkom inventaru, dokumentacije o konfiguracijama programskih proizvoda i opreme, te odgovornosti dionika IT sustava su osnovne pretpostavke za operativno stabilna stanja IT arhitekture na svim razinama zdravstvene zaštite.

Nadzor elemenata informatičkog sustava

Znanja o relacijskim bazama podataka elementarne su vještine za upravljane golemom količinom podataka koja nastaje u zdravstvenom sustavu. Kopiranje, arhiviranje i restauriranje redovite su dnevne obveze. Nadzor IT i IoT (engl. Internet of Things) moguće je samo uz potporu upotrebe SIEM rješenja (eng. Security Information and Event Management), sustava za prikupljanje, normalizaciju i automatiziranu analizu sigurnosnih

događaja i logova sa različitih uređaja u stvarnom vremenu. Nužan je automatiziran nadzor poslužitelja, skladišta podataka te radnih stanica i preklopnika. Pravovremena dostava informacija o stanju sustava također se može programski kontrolirati i usmjeriti, ali podjednako na sve sudionike sustava nadzora sistema.(2,3).

Suvremene zdravstvene organizacije suočavaju se s različitim izazovima

Sveprisutnost elektroničkih zdravstvenih zapisa je ogroman korak u poslovanju zdravstvenih ustanova. Digitalni podaci olakšavaju pristup i dijeljenje medicinskih informacija što direktno utječe na povećanje kvalitete skrbi za pacijente što stvara niže troškove poslovanja kroz povećanje učinkovitosti. Međutim, oni također stvaraju više odgovornosti oko upravljanja podacima i zaštitom podataka pacijenata od krađe, gubitka ili ometanja pristupa. Sada, osim aktivnog radnog sustava, moramo imati u pripremi i adekvatno rješenje u slučaju zastoja rada sustava, zbog bilo kojeg razloga. Ključno je da informatičari moraju osigurati tečno i kontinuirao poslovno radno okruženje a u slučaju havarije brz i adekvatan odgovor.

Osnovne pretpostavke s kojima se zdravstvena ustanova mora suočiti kod planiranja i izrade *Disaster Recovery plana i Business Continuity (BC&DR):*

1. *Kliničarima je potreban brz pristup podacima o pacijentima u svakom trenutku*

Katastrofe i neočekivani tehnološki zastoji su naša realnost. Kontinuitet poslovanja je posebno važan za funkcioniranje zdravstvenih ustanova; važno je u slučaju bilo kakvog tehnološkog incidenta u što kraćem roku omogućiti nastavak procesa s točnim i ažuriranim podacima o pacijentima, te poslovnim informacijama.

2. *Propisi i zahtjevi*

Zbog osjetljive prirode zdravstva širok raspon propisa i zakona obvezuju kako će i na koji način ustanova obrađivati osobne podatke pacijenata. Na primjer *GDPR* definira provođenje mjera zaštite podataka koji utječu na svaki segment rada, od bolesničkog kreveta do poslovnih partnera. A to je samo jedan od propisa i zakona koje treba poštivati.

3. *Big Data* i *BYOD* novi aspekt koji ima sve veći utjecaj

Vezano uz navedeno treba dodati činjenicu da je količina podataka o pacijentima s kojima se raspolaže ogromna i brzo raste, pogotovo kada je u pitanju zdravstvo i arhiviranje slika, te komunikacijski sustavi (HL7). Podaci se nalaze u informacijskom sustavu zdravstvene ustanove, no u današnje vrijeme i na tabletima, prijenosnim računalima ili pametnim telefonima zdravstvenih djelatnika, ne samo liječnika. Prema nedavnim anketama u zdravstvenom sustavu, 66% ispitanika vjeruje da uporaba vlastitih uređaja u poslovne svrhe *(BYOD)* znači budućnost pružanja zdravstvene skrbi i brige za pacijente. Istovremeno, potrebe za izradom sigurnosne kopije podataka (engl. backup/restore) rastu eksponencijalno, jer se mnogi zdravstveni podaci moraju čuvati do nekoliko godina, a neki i trajno zbog statističko planskih obrada podataka u javno zdravstvenim servisima države ili pokrajine.

4. *Proračun ne raste jednako brzo kao potrebe za zaštitom zdravstvenih informacija*

Zdravstvo je posao pa je stalno prisutna percepcija da uprava uvijek mora inzistirati na smanjenju troškova. Zdravstveni sustav se stalno razvija, stižu novi procesi i tehnologije, nove smjernice i preporuke za optimalan rad zdravstvenog sustava. I radna okolina, koje se temelji na IT infrastrukturi mora imati realnu i adekvatnu financijsku konstrukciju. Optimalno je da

financije prate tehnološki rast jer se povećava kvaliteta liječenja u zdravstvenom sustavu. Eksponencijalan rast količine multimedijskih podataka, posljedično slijede izazovi skladištenja i zaštite podataka. Tu su danas prisutne i sve novije i perfidnije tehnološke ugroze osim samih elementarnih nepogoda. Prvenstveno se misli na krađu podataka, što je vrlo sofisticiran i ozbiljan izazov za poslove iz portfelja informatičara 21 stoljeća. Zato je neophodno na vrijeme osigurati financijska sredstava, i za poslove i aktivnosti, nakon što se prođe prvi krug planiranja i implementacije *BC&DR-a.*

5. *Postoji bolji način*

Svi ti čimbenici povećavaju pritisak na cijelu organizaciju - posebice IT - kako bi se osigurao *BC&DR* koji odgovaraju na sve navedene izazove. To je vodilja za zdravstvene ustanove da se iznađe način kako osigurati kontinuitet poslovanja, te osigurati nesmetano liječenje pacijenata. IT permanentno traži nove načine za primjenu troškovno učinkovitih, ali robusnih, sigurnih i skalabilnih rješenja za *BC&DR*. Mnogi od njih fokusiraju se na *cloud* kako bi razvili dosljednu, centraliziranu i standardiziranu arhitekturu sigurnosnog kopiranja i obnavljanja oštećenih podataka. Cilj je smanjiti ili eliminirati nepotrebne troškove i smanjiti rizike poslovanja. Kvalitetnom prevencijom do optimalnih poslovnih uvjeta za poslovanje - to je misija IT. Premještanje poslovanja u oblak nije odluka koju treba uzeti olako. Da bi se dobilo maksimalnu korist od strategije poslovanja u oblaku, ona mora biti osmišljena u svjetlu specifičnih zahtjeva i mogućnosti organizacije. I prije nego što se počne razmišljati o tranziciji u oblak, mora se razumjeti što uključuju usluge u oblaku za zdravstvo, a vezano uz *BC&DR*.

6. Cloud Business Continuity & Disaster Recovery za zdravstvo

Mnoge zdravstvene organizacije trenutno koriste *BC&DR* unutar tvrtke pomoću traka i drugih fizičkih medija, skladište podataka ili NAS. No, posljednjih godina, poboljšanja u sigurnosti oblaka, zajedno s nevjerojatnim povećanjem količine multimedijskih medicinskih podataka koji se moraju pohraniti i zaštititi, navela su zdravstvene ustanove da razmisle o korištenju oblaka za neke aspekte *BC&DR*-a. Neki od glavnih razloga uključuju:

Zakonsku usklađenost

Prelazak na oblak s pružateljem usluga koji je certificiran i dobro upućen u zahtjeve zdravstvene industrije osigurava poštivanje važećih i novih propisa (4).

Bolje ciljeve oporavka

Iako će *„offsite“*, izvanmrežni ili fizički medijski prostor za pohranu štititi podatke, ta rješenja nude ciljeve vremena oporavka (RTO) od nekoliko sati do nekoliko dana i ciljeve oporavka točke (RPOs) od jednog dana ili više, ovisno o rasporedu sigurnosnog kopiranja. Iako su mrežne sigurnosne kopije najbrže za vraćanje, u slučaju velike katastrofe također se mogu izgubiti i mrežne sigurnosne kopije. Kako bi ublažili taj rizik, sigurnosne kopije koje se nalaze u oblaku, iako nešto sporije za povrat ulaganja (RTO), pružaju zaštitu koja može biti vrijedna kompromisa ovisno o specifičnim zahtjevima.

Premještanje rashoda iz *CAPEX*-a u *OPEX*

Prebacivanje inicijativa *BC&DR*-a iz kapitalnih izdataka - vezanih uz kupnju opreme - za operativne troškove putem modela usluge u oblaku donosi višestruke koristi, uključujući niže početne troškove, predvidivost proračuna i mogućnost da se 100% troškova nadoknadi putem izvješća o troškovima.

Brza implementacija i poboljšana skalabilnost

Ugovorni pružatelj usluga u oblaku može vrlo brzo osigurati resurse za zdravstvenu ustanovu. Konfiguracije se mogu vrlo lako povećavati ili smanjivati prema potrebi s ogromnom fleksibilnošću.

Prelazak poslovanja u oblak

Uz usluge u oblaku, *može se osloniti na stručnog partnera koji je dobro upućen u tehničke aspekte BC*&DR-a, koji ispunjava zahtjeve za povećanjem performansi, sigurnosti, prostora za pohranu, zahtjevima troškova. Također mogu se smanjiti troškovi vezani uz osoblje i podršku internih operacija i pustiti IT odjelu da se usredotoči na inicijative koje poboljšavaju skrb o pacijentima. Glavna je funkcija IT da unapređuje poslovne procese uvođenjem novih IT rješenja, što direktno utječe na povećanje kvalitete života u lokalnoj zajednici.

Najbolje prakse u BC&DR za zdravstvene organizacije

Oblak nudi brojne koristi za *BC&DR*, a tehnologija u oblaku i sigurnosne tehnike napreduju do razine na kojoj je oblak još sigurniji od neovlaštenih upada i gubitaka nego vlastiti podatkovni centar. Prednosti prebacivanja *BC&DR*-a u oblak su mnoge, a zdravstvo ima vrlo posebne zahtjeve na ciljeve zaštite podataka i oporavka. Osiguravanje da se dobije pravo rješenje zahtijeva formalni pristup u odabiru i provjeri rješenja.

Procjena spremnosti ustanove za izbor optimalne implementacije rješenja i mapiranje potrebnih poslovnih procese može se deklarirati sljedećim koracima:

Prvi korak: provjeriti postojeće *BC&DR* okruženje

Najbolji način za početak planiranja *BC&DR* strategije koja adekvatno štiti podatke je put IT revizije. To će pomoći kritički procijeniti postojeće stanje, što dobro radi, što treba poboljšati, jasno navodeći postojeća i kratkoročna pitanja. Detaljan revizijski pregled uključuje sljedeće:

1. Provjera procjene rizika

Procijeniti rizik za ustanovu znači utvrditi što se događa ako bilo koja važna poslovna aplikacija postane nedostupna. Prilikom izrade studije treba voditi računa o mogućnosti lokalnog oporavka u odnosu na mogućnosti daljinskog oporavka. Daljinski oporavak će po prirodi proširiti *RTO*, osim ako okruženje nije zaštićeno tehnologijom replikacije u odnosu na sigurnosne kopije podataka.

Procjena rizika uključuje:

- Identificirati sve kritične aplikacije
- Izračunati klinički rizik za svaku aplikaciju ako je došlo do prekida rada
- Izračunati učinak, u kunama/EUR, za svaku aplikaciju ukoliko je došlo do prekida rada
- Dokumentirati kako je svaka sigurnosna kopija zaštićena
- Odrediti koliko će trajati oporavak svake aplikacije pod trenutnom strategijom BC&DR-a
- Odrediti željeni *RTO* i *RPO* za svaku aplikaciju/sustav
- Usporediti željene *RTO* / *RPO* ciljeve s trenutnim stanjem da odredimo raspone
- Dokumentirati spremnost procedura prekida rada, uključujući obuku i testiranje

Slika 3. Kontinuitet poslovanja i planiranje oporavka; Izvor: https://searchdisasterrecovery.techtarget.com/Data-center-disaster-recovery-plan-template-and-guide

2. Provjera izvedbe IT-a

Provjera izvedbe IT-a zahtijeva ispitati brzinu i učinkovitost trenutnog sustava za izradu sigurnosnih kopija i oporavak kako bi se identificiralo uska grla i strategije poboljšanja. Posebne provjere uključuju osiguranje:

- Podaci se pohranjuju na vlastitoj infrastrukturi
- Interno IT osoblje ispunjava sporazume na operativnoj razini (OLA)
- *RTO / RPO*-ovi su uspostavljeni po zahtjevu, a plan oporavka se prati kako bi se postigli ili premašili ovi ciljevi

3. Provjera sigurnosne kopije

Provjera sigurnosne kopije zahtijeva analizirati datotečne sustave i baze podataka kako bi se utvrdilo jesu li podaci u opasnosti.

Specifični koraci uključuju:

- Praćenje uspješnosti i neuspješnosti sigurnosnih kopija
- Praćenje i rješavanje neuspjelih sigurnosnih poslova
- Osiguravanje sigurnosnih kopija nadoknađuje se testiranjem

- Provjera mogućnosti oporavka granulirane su na razini datoteke
- Osiguravanje da su podaci zaštićeni "kriptirani", tj. kodirani na mediju za pohranu ili ciljnom mediju/lokaciji

4. Vratiti provjeru mogućnosti

Ovo je vrijeme za procjenu BC&DR planova kako bi se utvrdilo postoje li pravi procesi i sposobnosti za vraćanje podataka i sustava u slučaju bilo kakvog incidenta ili situacije deklarirane kao prirodne katastrofe.

Posebne provjere uključuju:

- Osiguravanje postojanja formalnog plana oporavka, uključujući prelazak s procedura prekida rada na informacijske sustave i potrebnu „resinkronizaciju“
- Redovito testiranje *BC&DR* sustava i procesa putem živih testova i scenarija
- Analiza operativnih postupaka oporavka
- Ocjenjivanje integriteta podataka i spremnosti za oporavak, uključujući slijed ili obnavljanje i vraćanje sučelja
- Izvršiti analizu nedostataka ciljeva oporavka u odnosu na mogućnosti
- Osigurati da je u sustave ugrađena redundantnost
- Identificiranje novih aplikacija u okruženju i ažuriranje procjene rizika
- Identificiranje svih umirovljenih sustava i potvrda da su uklonjeni s *BC&DR* platforme i plana

5. Druga razmatranja

- Koliko vremena IT osoblje posvećuje rezervnim aktivnostima?
- Postoji li potreba za zanavljanjem opreme ili drugi IT kapitalni izdaci?
- Tražimo li dodavanje više prostora za pohranu u bliskoj budućnosti?

Odgovori na ova pitanja daju bolji uvid u to kako prelazak u oblak može koristiti organizaciji u vrlo specifičnim područjima. Na kraju ovog pregleda zdravlja IT sustava nastaje jasna snimka trenutnih mogućnosti i razumijevanje gdje treba povećati učinkovitost i pouzdanost sigurnosnih sustava i obnoviti procedure.

Drugi korak: Izvršiti analizu utjecaja

Premještanje BC&DR operacija u oblak je proces koji se može provoditi u više koraka. Prvo se odredi koje aspekte poslovnih operacija trebate premjestiti u oblak i kada. To se radi analizom utjecaja. Ovo je važna vježba koja pomaže odrediti koje su funkcije najkritičnije za organizaciju i koje će pomoći voditi strategiju usvajanja.

Počinje se s definiranjem troškova, koristi i rizika povezanih s pomicanjem aspekata BC&DR-a u oblak. Svakako treba razmotriti sljedeće glavne točke utjecaja:

- Financijski / proračun
- Osoblje
- Tehnologija
- Poslovni procesi
- Usklađenost
- sigurnosti
- Njega bolesnika / klinički
- Inovacija / rast
- Ostali elementi koje odredite od ključne su važnosti za organizaciju.

To daje jasnu sliku o trenutnom stanju spremnosti za oblak i dovodi do strategije korak-po-korak za premještanje u oblak označavanjem:

- *BC&DR* elemenata koji mogu odmah migrirati radi neposredne koristi
- *BC&DR* elemenata koji mogu migrirati u bliskoj budućnosti
- *BC&DR* elementi koji možda nisu dobar kandidat za oblak u ovom trenutku, ali mogu biti u budućnosti u skladu s promjenama u poslovnom okruženju .

Premještanje svih aktivnosti sigurnosnog kopiranja u oblak može imati pozitivan utjecaj na sve navedene točke s vrlo malo nedostataka što ga čini dobrim kandidatom za prelazak na oblak odmah. Premještanje kontinuiteta poslovanja u oblak može zahtijevati više pripreme zbog utjecaja tehnoloških, kadrovskih i poslovnih procesa.

Treći korak: Objasniti zahtjeve rješenja

Kada se utvrdi koji su postupci dobri kandidati za oblak, može se početi prikazivati zahtjeve rješenja. Svako novo rješenje ima utjecaj na organizaciju iz poslovne perspektive i IT perspektive, stoga treba prikupiti zahtjeve svakog skupa dionika. Mora se opisati zahtjeve sa što je moguće više pojedinosti, uključujući:

- *RTO / RPO* ciljeve za specifične primjene
- Sve zahtjeve za sigurnosno kopiranje specifični za aplikaciju
- Regulatorne zahtjeve koji utječu na pružatelje usluga u oblaku (ugovor o poslovnim suradnicima, certifikat visoke dostupnosti, sigurnosni certifikati itd.)
- Osiguranje da su podaci zaštićeni u pokretu i mirovanju
- Očekivanja oko BC&DR testiranja i sanacije
- Rokove implementacije rješenja
- Potrebne značajke kao što su:
    - Mogućnost sigurnog dijeljenja podataka unutar vlastite mreže
    - Podrška za mobilnost i BYOD
    - Sposobnosti pretraživanja i vraćanja u segmentima
- Zahtjeve resursa kao što su:
    - Zahtjevi IT resursa
    - Zahtjevi troškova / proračuna

Rezultati ove vježbe mogu činiti osnovu zahtjeva za prijedlog (RFP) koji se može poslati dobavljačima kako bi mogli izravno odgovoriti na zahtjeve specifičnim informacijama o njihovim mogućnostima. Treba biti oprezan i pažljiv kada se pravi popis zahtjeva za rješenje na temelju vlastitih kriterija jer u izradi BC&DR plana ne postoji copy/paste. Svaka je ustanova u većini slučajeva specifična.

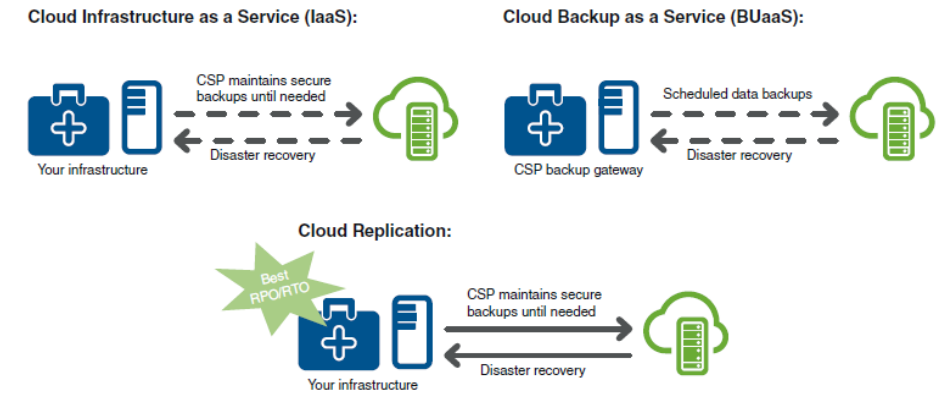
Četvrti korak: mapiranje svojih zahtjeva prema dostupnim modelima implementacije

Ova je točka vrijeme da se uskladi zahtjeve rješenja s različitim vrstama dostupnih rješenja u oblaku. Postoje razne dostupne opcije od potpuno „in-house“ rješenja za privatni oblak do rješenja s pružateljem usluga u oblaku i pristupnim točkama između njih. Idealan scenarij za organizaciju može biti mješoviti pristup koji se temelji na funkcionalnosti. Ako je cilj vratiti izgubljenu datoteku ili samo jedan poslužitelj, vrlo dobro mogu poslužiti lokalne ili sigurnosne kopije iz oblaka. Ako je cilj prije svega zaštititi podatke i sustave, sigurna kopija podataka (backup) u oblaku je idealno rješenje. Ako je cilj brzi oporavak sustava za vraćanje funkcionalnosti krajnjim korisnicima, imamo rješenje za replikaciju u oblaku.

Koji se tip rješenja odabire ovisi o korisničkim jedinstvenim zahtjevima. Kao primjer može se navesti želja da se zadrži kontrola nad određenim aspektima svoje strategije, dok premještanje svega drugoga, kao što je sigurnosna kopija, u oblak može odmah (5).

Neke opcije uključuju:

- *Cloud Infrastructure-as-a-Service* (IaaS): Ova usluga u oblaku nudi udaljeno sigurno spremište za sigurnosne kopije podataka. Posjeduje se i upravlja vlastitim softverom i hardverom za sigurnosno kopiranje te jednostavno šalje kopije podataka davatelju usluga u oblaku, a zatim se te podatke preuzima prema potrebi. Ovim kompletnim rješenjem za „backup“ upravlja i posjeduje naša ustanova.
- *Cloud Backup-as-a-Service* (*BUaaS*): U ovom scenariju, dobavljač isporučuje cjelovito rješenje za sigurnosno kopiranje na vašoj web-lokaciji koje pruža mogućnost nadilaženja grešaka u njihovom podatkovnom centru u oblaku. Posjeduju i upravljaju cijelim procesom od početka do kraja.
- Replikacija u oblaku: Ako imamo kritične sustave kojima je potrebna maksimalna zaštita s kratkim *RTO*-om i malim gubitkom na RPO-u, morat će se razmotriti replikacija za razliku od sigurnosnih kopija. Replikacija će kontinuirano ažurirati podatke i stanje aplikacije u oblaku pružajući najagresivniji plan za brzi oporavak. Iskusni pružatelj usluga u oblaku zdravstvene skrbi može pomoći razumjeti nijanse i osmisliti najbolju kombinaciju modela implementacije za vaše potrebe.



Slika 4. Sigurnosne opcije

Peti korak: Odrediti kriterije odabira dobavljača

Kada se zna što se traži, vrijeme je da se uskladi ponude dobavljača sa svojim zahtjevima. Očekuje se da će dobavljači odgovoriti na sve zahtjeve, a zatim suziti polje na temelju kriterija kao što je mogućnost dobavljača da:

- Pokaže iskustvo i stručnost u zdravstvenoj industriji uključujući zakonske usklađenosti, visoku razinu pouzdanosti i spremnost da potpišu najvišu razinu dostupnosti i kvalitete usluge
- Osigura Tier III okruženje podatkovnih centara koji je certificiran s obzirom na SOC II i III i SAEE 16
- Jamstveni ugovori na razini usluge
- Osiguravanje postavljenog vremena odgovora, ovisno o riziku za organizaciju (vrlo hitno, hitno, standardno itd.)
- Navođenje ciljeva *RTO* i *RPO* koji zadovoljavaju smjernice za procjenu rizika
- Isporučivanje 24x7x365 podršku za zdravstvenu zaštitu uživo
- Brzo pružanje dodatnih usluga po potrebi
- Omogućavanje testiranja postojećih rješenja prije izvršenja
- Dostava preporuke kako bi se maksimalno povećalo povrat ulaganja u pohranu

- Mogućnost kriptiranja podataka pohranjenih u oblaku najnovijim tehnologijama kao što su kriptiranje cijelog fizičkog diska, virtualnog diska ili enkripcija datoteka / mapa

Zaključak

Kada se razmišlja o promjeni strategije *BC&DR*-a potreban je siguran odgovor na pitanje: "Jesmo li spremni prebaciti neke ili sve *BC&DR* sustave/podatke u oblak?"

S poslovne strane moraju se stvoriti uvjeti za standardne poslovne karakteristike:

1. Kontinuirano visok standard skrbi o pacijentima
   - Održavanje sigurnosti da su točni, ažurni podaci o pacijentima dostupni zdravstvenom osoblju u svakom trenutku, u više ustanova na svoj opremi koja se koristi u obradi podataka
   - Zaštita organizacije od odgovornosti i novčanih kazni koje mogu biti posljedica nepoštivanja zakonskih odredbi
   - Upravljanje proračunom s osvrtom na donju granicu.

2. S tehničkog stajališta predloženo operativno rješenje omogućava podršku navedenim poslovnim ciljevima, što uključuje:
   - Izradu sigurnosnih kopija i obnavljanje ogromnih količina podataka
   - Optimiziranje zahtjeva za propusnost
   - Rad u okviru proračunskih ograničenja IT-a
   - Zaštitu podataka u mirovanju, mrežnom prometu, te razmjeni između raznih sustava i uređaja
   - Odabir najbolje metode za spremanje i vraćanje sustava i podataka, kako bi se osigurao kontinuitet poslovanja u slučaju katastrofe.

Rješenje koje zadovoljava i poslovne i tehnološke izazove omogućit će održavanje usklađenosti sa zakonskim smjernicama, čime se pruža i omogućuje briga za sve sudionike u poslovnim procesima u zdravstvenom sustavu uz pojednostavljenje IT upravljanja i smanjenje kapitalnih izdataka. Koliko će sustava preseliti u oblak ovisit će o zahtjevima organizacije, potrebi i spremnosti. Koristeći navedene korake može se bolje razumjeti gdje se nalazite, gdje trebate biti i kako stići tamo.

Planiranje i izrada *Disaster Recovery i Business Continuity* plana (BC&DR) zahtjeva znatna financijska ulaganja, multidisciplinarni pristup, stručni i osposobljeni kadar, te podršku rukovodstva bolnice. Već i manje bolnice su dovoljno kompleksni sustavi gdje bi izrada takvog plana trajala nekoliko mjeseci. Zbog svega navedenog bolnice nemaju kapaciteta da samostalno izrade *BC&DR* plan niti da implementiraju rješenja iz plana. To su poslovi za informatičku struku koja ima jasna znanja i kompetencije da provede u život takve projekte. I zakoni o zaštiti osobnih podataka, kibernetičkoj sigurnosti, o medicinskim podacima jasno ukazuju da informatičari imaju sposobnost provesti planirano i zakonom utvrđeno u realne okvire i aplicirati u poslovne aplikacije. Moguće je da te poslove u kooperaciji s internim informatičarima u bolnicama optimalno odrade specijalizirane vanjske firme koje proces *BC&DR* mogu posložiti u praksi. Većina bolnica u Hrvatskoj ima relativno dobro razrađen infrastrukturni sloj, no treba ozbiljno poraditi na ostalim slojevima *BC&DR* infrastrukture.

Literatura

1. Witten IH, Frank E, Hall MA, Pal CJ. Data Mining, Practical Machine Learning Tools and Techniques. Amsterdam: Morgan Kaufmann 2017, Fourth Edition,
2. Deloach D, Berthesen E, Elrifai W. The Future of IoT: Leveraging the Shift to a Data Centric World. BookBaby 2017.
3. Pomper D, Pomper S. Odjel za informatiku OB Varaždin – primjena Zakona o provedbi opće uredbe za zaštitu osobnih podataka u zdravstvenom prostoru RH. Medix 2018; 24(132).
4. Perinović V, Škarecki C, Pomper D, Pomper S. Kako znanje informatičara štiti ugled zdravstvene struke. Medix 2018; 24(133/134).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Ovaj tekst je napisan s namjerom da pomogne u razvijanju svjesnosti i spremnosti i donošenju optimalne odluke za tip implementacije u zdravstvenoj ustanovi i popis potrebnih koraka da se tamo stigne.