UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

IMPLEMENTACIJE TEHNOLOGIJA ZA KONTINUIRANI KOMPJUTING: KOMPARATIVNA ANALIZA

Sarajevo, juni 2024. VILDAN BEŠIREVIĆ

U skladu s članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se

IZJAVA O AUTENTIČNOSTI RADA

Ja, Vildan Beširević, student drugog (II) ciklusa studija, broj index-a 4816 na programu Menadžment, smjer Menadžment i informacione tehnologije, izjavljujem da sam završni rad na temu:

IMPLEMENTACIJE TEHNOLOGIJA ZA KONTINUIRANI KOMPJUTING: KOMPARATIVNA ANALIZA

pod mentorstvom prof. dr. Nijaza Bajgorića izradio samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija, uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predao elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web-stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu s članom 34. 45. i 46. Zakona o autorskom i srodnim pravima („Službeni glasnik BiH“, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 01.06.2024. Potpis studenta:

SAŽETAK

U ovom radu detaljno su proučeni koncepti kontinuiteta poslovanja i kontinuiranog kompjutinga. Pojašnjena su značenja i bitne karakteristike ovih pojmova, što uključuje važnost kontinuiteta poslovanja u sprečavanju i upravljanju rizicima te osiguravanju stabilnosti organizacije u slučaju neočekivanih događaja. Dat je i historijski osvrt na razvoj kontinuiranog poslovanja i kompjutinga, kako bi se stekao bolji uvid u evoluciju ovih disciplina te razumjelo kako su se prilagođavali tehnološkim promjenama tokom vremena.

Predstavljene su različite strategije, pristupi i najbolje prakse upravljanja kontinuitetom i rizicima poslovanja. Također, istražena je tematika oporavka od katastrofa, što uključuje planiranje i implementaciju procedura i rješenja za brzi oporavak.

Cilj ovog rada je da pruži uvid u različite aspekte implementacije tehnologija za kontinuirani kompjuting, s fokusom na server-računare, server operativne sisteme, baze podataka, tehnologije za *backup* podataka, računarske mreže, *cyber*-sigurnost, *cloud computing* i virtualizaciju, kao i druge, nove tehnologije koje su relevantne za kontinuitet poslovanja. U sklopu ovoga rada prezentovana je i komparativna analiza različitih tehnologija za kontinuirani kompjuting, bazirana na općoj slici prednosti i nedostataka ovih tehnologija u kontekstu performansi, energetske efikasnosti, pouzdanosti, sigurnosti, kompleksnosti, skalabilnosti i fleksibilnosti svake tehnologije.

Ključne riječi: kontinuitet poslovanja, kontinuirani kompjuting, upravljanje kontinuitetom poslovanja, planiranje kontinuiteta poslovanja, oporavak od katastrofe, upravljanje rizicima u poslovanju, tehnologije za kontinuirani kompjuting.

ABSTRACT

In this paper, the concepts of business continuity and continuous computing are studied in great detail. The meanings and essential characteristics of these terms are clarified, which includes the importance of business continuity in preventing and managing risks and ensuring the stability of the organization in case of unexpected events. A historical overview of the development of business continuity and continuous computing is also presented, in order to gain a deeper insight into the evolution of these disciplines and understand how they have adapted to technological changes over time.

Different strategies, approaches and best practices of business continuity and risk management are presented. Also, the topic of disaster recovery was explored, which includes planning and implementation of procedures and solutions for rapid recovery.

The aim of this paper was to provide an insight into various aspects of the implementation of technologies for continuous computing, with a focus on server computers, server operating systems, databases, data backup technologies, computer networks, cyber security, cloud computing and virtualization, as well as other new technologies which are relevant for

business continuity. As part of this paper, a comparative analysis of different technologies for continuous computing is presented. Comparative analysis is based on the general overview of advantages and disadvantages of these technologies in the context of performance, energy efficiency, reliability, security, complexity, scalability and flexibility of each technology.

Keywords: business continuity, continuous computing, business continuity management, business continuity planning, disaster recovery, business risk management, technologies for continuous computing

SADRŽAJ

1. UVOD **1**
1.1. Predmet i problem istraživanja **4**
1.2. Svrha i ciljevi istraživanja **4**
1.3. Istraživačka pitanja i hipoteze **4**
1.4. Metodologija istraživanja **5**
1.5. Struktura rada **6**
2. KONTINUITET POSLOVANJA I KONTINUIRANI KOMPJUTING **6**
2.1. Pojmovi kontinuitet poslovanja i kontinuirani kompjuting **6**
2.2. Historijski osvrt i razvoj kontinuiteta poslovanja i kontinuiranog kompjutinga **8**
2.3. Upravljanje kontinuitetom poslovanja i planiranje **11**
2.4. Oporavak od katastrofe **15**
2.5. Upravljanje rizicima u poslovanju **16**
3. IMPLEMENTACIJE TEHNOLOGIJA ZA KONTINUIRANI KOMPJUTING: KOMPARATIVNA ANALIZA **17**
3.1. Server-računari **18**
3.2. Server operativni sistemi **19**
3.3. Baze podataka i tehnologije za backup podataka **22**
3.4. Računarske mreže **27**
3.5. Cyber-sigurnost **32**
3.6. Cloud computing i virtualizacija **37**
3.7. Ostale nove tehnologije **41**
3.7.1. „Internet stvari“ (engl. *Internet of Things* – IoT) 42
3.7.2. „Edge“ računarstvo (engl. *Edge computing*) 43
3.7.3. „Spremnici“ (engl. *Containers*) 44
3.7.4. Oporavak od katastrofe kao usluga (engl. *Disaster Recovery as a Services*) 46
3.7.5. 5G mreža 47
3.8. Komparacija koncepata kontinuiranog kompjutinga 49
3.8.1. Komparacija koncepata 54
4. ZAKLJUČAK 60
REFERENCE 63

POPIS TABELA

Tabela 1. Komparacija redudantnih server-računara 18
Tabela 2. Komparacija server operativnih sistema 20
Tabela 3. Komparacija backup tehnologija 23
Tabela 4. Komparacija tehnologija računarskih mreža 29
Tabela 5. Komparacija tehnologija za cyber-sigurnost 34
Tabela 6. Komparacija cloud computing tehnologija 39
Tabela 7. Komparacija IoT tehnologije 42
Tabela 8. Komparacija edge computing tehnologije 44
Tabela 9. Komparacija containers tehnologije 45
Tabela 10. Komparacija DRaaS tehnologije 47
Tabela 11. Komparacija 5G tehnologije 48
Tabela 12. Komparacija metoda mjerenja performansa 53
Tabela 13. Komparacija koncepata 55
Tabela 14. Komparacija mjerljivosti atributa koncepata 57
Tabela 15. Komparacija parametara 58

POPIS SLIKA

Slika 1. Taksonomija koncepta “Dependability” 49
Slika 2. Taksonomija koncepta “Fault-Tolerance” 50
Slika 3. Taksonomija koncepta “Reliability” 51
Slika 4. Taksonomija koncepta “Security” 52
Slika 5. Taksonomija koncepta “Survivability” 53
Slika 6. Odnos između koncepata 56
Slika 7. Hijerarhija i međuzavisnost koncepata 56
Slika 8. Metoda evaluacije koncepata 59

POPIS SKRAĆENICA

BC - business continuity (kontinuitet poslovanja)
BCI - Business Continuity Institute (Institut za kontinuitet poslovanja)
BCM - business continuity management (menadžment kontinuiteta poslovanja)
BCP - business continuity planning (planiranje kontinuiteta poslovanja)
BIA - business impact analysis (analiza utjecaja na poslovanje)
CAD - computer-aided design (kompjuterski potpomognt dizajn)
CAM - computer-aided manufacturing (kompjuterski potpomognta proizvodnja)
CAPS - computer-aided planning systems (kompjuterski potpomognta sistem za planiranje)
CRM - customer relationship management (sistema za upravljanje odnosima s klijentima)
DLP - data loss prevention (sprečavanje gubitka podataka)

DNS - domain name system (sistem naziva domena)
DR - disaster recovery (oporavak od katastrofe)
DRaaS - disaster recovery as a services(oporavak od katastrofe kao usluga)
ERP - enterprise resource planning (sistema za planiranje resursa preduzeća)
GIS - geografski informacioni sistem
IaaS - infrastructure as a service (infrastruktura kao usluga)
IDPS - intrusion detection and prevention system (sistem za detekciju i prevenciju upada)
IKT - informacijska i komunikacijska tehnologija
IoT - Internet of Things (internet stvari)
LAN - local area network (lokalna mreža)
LB - load balancer (balanser opterećenja)
NMS - network management systems (sistemi za upravljanje mrežom)
PaaS - platform as a service (platforma kao usluga)
PAM - privileged access management (upravljanje privilegovanim pristupom)
PC - personal computer (personalni računar)
RAID - redundant array of independent disks (redundantni niz nezavisnih diskova)
RPO - recovery point objective (cilj tačke oporavka)
RTO - recovery time objective (cilj vremena oporavka)
SaaS - software as a service (softver kao usluga)
SAN - storage area network (skladišna mreža)
SIEM - security information and event management (upravljanje događajima i sigurnosnim informacijama)
SPOF - single point of failure (pojedinačna tačka kvara)
VPN - virtual private network (virtuelna privatna mreža)
WAF - web application firewall (firewall za web aplikacije)
WAN - wide area network (širokopojasna mreža)

1. UVOD

Kroz historiju, čovjek je uvijek težio usavršavanju i upotpunjavanju. Primitivne alate zamijenile su visokosofisticirane i kompleksne tehnologije koje su postavile temelj i omogućile razvoj savremenog društva. Paralelno s tim, razvijali su se kultura, nauka i međuljudski odnosi, a sve to je potpomogla uspješna ekonomija. Kao takva, ekonomija je pretrpjela razne preobrazbe kako bi se našao najbolji, optimalan način za uspješno poslovanje i saradnju. Međutim, prijetnje i rizici uvijek su postojali bez obzira na nivo razvijenosti ekonomije. Pronalazili su se različiti načini kojima bi se smanjio utjecaj negativnih, nepredvidivih događaja i ostvario nastavak u radu i poslovanju. Danas, kao rezultat kumulativnog razvoja, moderne kompanije inkliniraju i posežu za alatima i procesima koje definiše koncept *kontinuitet poslovanja* (engl. *business continuity* - BC).

Kontinuitet poslovanja predstavlja mogućnost kompanije da nastavi s poslovanjem u slučaju nesreća ili incidenata koji direktno utječu na proizvodnju i isporučivanje proizvoda i usluga. Da bi kompanija u tim okolnostima uspjela održati zadovoljavajući nivo poslovanja, potrebno je *planirati kontinuitet poslovanja* (engl. *business continuity planning*). To predstavlja proces kreiranja plana i mehanizama koji će spriječiti nepoželjne prijetnje, te kreiranje plana za oporavak od katastrofe (engl. *disaster recovery* - DR).

Karim (2011) pojašnjava da je plan oporavka od katastrofe zapravo način na koji će kompanije odgovoriti na sve interne ili eksterne događaje, kako bi osigurale kritične operacije u cilju smanjenja posljedica katastrofa te eventualne zaštite dobara i imovine.

Bitno je naznačiti da planiranje kontinuiteta poslovanja i oporavak od katastrofe nisu isto. Stanton (2005) u svom članku pod nazivom „Beyond disaster recovery: the benefits of business continuity“ navodi kako se plan oporavka od katastrofe obično primjenjuje kao proces koji se dešava prije i nakon same katastrofe, a primarno se odnosi na IT sisteme, dok planiranje kontinuiteta poslovanja predstavlja proces kojim se osigurava poslovanje kompanije, tako da se može održati i nastaviti neometano. Dakle, razlika je u tome što je planiranje kontinuiteta poslovanja zapravo korak koji se poduzima prije nego što se katastrofa uopće desi, a oporavak od katastrofe slijedi poslije.

Speight (2011) tvrdi da kontinuitet poslovanja uspostavlja procese koji su ključni za kompaniju, a također definiše i određuje upravljanje resursima. Raspoređivanje resursa je od vitalne važnosti. Kroz implementaciju kontinuiteta poslovanja vrši se kontrola resursa unutar kompanije i određuju se vremenska ograničenja njihovog raspoređivanja na kritičnim funkcijama, jer takve funkcije imaju interne i eksterne obaveze prema vendorima, klijentima, raznim sistemima i proizvodnim pogonima. Zato je bitno da se kroz kontinuitet poslovanja analiziraju i definišu kritične operacije i resursi te se rangiraju prema prioritetima.

Održavanje kontinuiteta poslovanja ne oslanja se samo na planiranje, nego i na menadžment kontinuiteta poslovanja (engl. *business continuity management* - BMC). Sapapthai i saradnici (2020) definišu menadžment kontinuiteta poslovanja kao proces koji se bazira na evaluaciji i procjeni utjecaja rizika i poslovanja kako bi kompanija postala otpornija na krizne situacije. Sapapthai i saradnici ističu da se u posljednjoj deceniji globalno povećava broj kriznih situacija, kako prirodnih tako i društveno-ekonomskih, što za posljedicu ima podizanje svijesti o važnosti menadžmenta kontinuiteta poslovanja.

Na kompanije mogu utjecati razne krizne situacije, tako Herbane (2010) ukazuje na to da kompanije mogu biti pogođene raznolikim katastrofama, poput prirodnih nesreća, nefunkcionalnih proizvoda, gubitka struje i vode, nestašice fosilnih goriva, prekida u komunikaciji, problema s ljudskim resursima, kriminalom, sabotažom, recesijom itd. Svaka od ovih situacija se može evidentirati i analizirati u sklopu menadžmenta kontinuiteta poslovanja.

Osim navedenih, Cerullo, V. i Cerullo, M. J. (2004) ističu da postoje i druge potencijalne katastrofe koje mogu biti izazvane usljed ljudske greške, kvara na pogonu ili instalacijama, malicioznih namjera i sl. Vjerovatnoća nastajanja smetnji u poslovanju raste zbog rizika koji uzrokuje sve viši nivo inkorporacije IT tehnologija i informacionih sistema u same kompanije, što podrazumijeva nove infrastrukture i uređaje koje je potrebno adekvatno održavati, a izloženost raste zbog eksternih umrežavanja. Tako raste opasnost od *cyber*-kriminala, koji podrazumijeva neovlašten pristup informacijama, softverima, sistemima i servisima, pa čak i raznim fizičkim uređajima koji se, usljed napada, može kompromitovati. Upravo zbog toga je nužno da kompanije imaju implementirane tehnologije koje omogućavaju kontinuitet poslovanja, to jest kontinuirani kompjuting.

Bajgorić (2006) navodi kako je kontinuirani kompjuting osnova za održavanje kontinuiteta poslovanja u savremenom dobu. Također ističe kako se moderne kompanije, koje svoje poslovanje zasnivaju na primjeni informacionih tehnologija, suočavaju sa zadatkom konstantne obrade podataka te visokog nivoa dostupnosti servisa i alata. Ono što kontinuirani kompjuting još osigurava jeste mogućnost krajnjim korisnicima da jednostavno i sigurno pristupaju svojim informacijama i servisima koristeći raznolike uređaje poput laptopa, računara i pametnih telefona. To, u konačnici, rezultira efikasnijim, bržim i kvalitetnijim odlukama u rješavanju svakodnevnih poslovnih problema i zadataka krajnjih korisnika ili kompanija.

Kompanije koje svoje poslovanje zasnivaju na informacionim sistemima su u vrlo specifičnoj poziciji, smatraju Asnar i Giorgini (2008), jer su današnji informacioni sistemi jako kompleksni i zahtijevaju visok nivo interakcije između čovjeka i sistema koji čine hardver, softver, korisnici, podaci itd. Tako je za kompanije koje svoje poslovanje zasnivaju na internet-servisima ili e-trgovinama, i koje su ovisne o internet-provajderima, od ključne važnosti održati poslovanje kroz kontinuirani kompjuting i menadžment kontinuiteta poslovanja.

Važnost informacionih sistema poentirali su Winkler, Gilani, Marshall i Guitman (2012). Oni ih definišu kao skupinu servisa, hardvera, softvera i mrežnih komponenti koje čine konfigurisan sistem koji izvršava poslovne operacije kompanije. Smetnje na tim sistemima direktno utječu na poslovanje, što može ostaviti i negativne finansijske i pravne posljedice te loše utjecati na cjelokupan ugled kompanije. Winkler i saradnici (2012) ističu kako je menadžment kontinuiteta poslovanja taj koji treba pronaći potencijalne prijetnje za informacione sisteme, kritične poslovne procese i resurse, IT servise, operacije te procijeniti štete i gubitke ako neki od elemenata otkaže. Ova analiza se drugačije zove i analiza utjecaja na poslovanje (engl. *business impact analysis* - BIA). Na osnovu te analize, stručnjaci na polju kontinuiteta poslovanja trebaju definisati koji su to prihvatljivi vremenski okviri unutar kojih kompanije trebaju realizovati normalan rad kako bi nastavile s poslovanjem. Winkler i saradnici (2012) također navode da je to veoma složen proces jer su IT sistemi kompleksni i unikatni s obzirom na to da svaki ima drugačije implementirane procese i tehnologije te svaki od njih ima specifičan način modeliranja tih procesa. Dodatno, IT sistemi se konstantno nadograđuju i mijenjaju. Tako i najmanja greška izmjene procesa može imati katastrofalne posljedice za kompaniju, a kod sofisticiranih sistema je to veliki problem budući da ne postoji osoba koja poznaje kompletan sistem u cijelosti.

Kontinuirani rad informacionih sistema, to jest kontinuirani kompjuting, usljed tih posljedica i katastrofa glavni je odgovor razvoja plana kontinuiteta koji osigurava IT servisima i organizacijama da se vrate normalnom nivou rada što je prije moguće, navodi Kassema (2020). Također, ističe kako je cilj tog plana smanjiti potencijalne štete i zaštititi glavne resurse pod kojima se podrazumijevaju razni uređaji, komponente, softver, hardver, informacioni sistemi, podaci i informacije koje sveobuhvatno vrše kontinuirani kompjuting. Lewis (2005) upozorava da brojne kompanije možda imaju neki vid plana koji osigurava kontinuirani kompjuting i informacione sisteme, ali se ipak dešavaju propusti zbog osjetljivosti mrežnih i informaciono-komunikacionih sistema, nedostupnosti ključnih ljudi i eksperata u datom trenutku, te pogrešne procjene prioritizacije ili neadekvatnog testiranja plana. Šimonova i Šprync (2011) ističu da greške na informacionim sistemima mogu imati velike posljedice u vidu direktnih troškova, neplaniranih radnih sati, gubitka već uloženih, te pada prihoda usljed gubitka reputacije i klijenata. Klijenti odlučuju promijeniti proizvod ili uslugu jer njihov vendor nije vršio monitoring svojih informacionih sistema na vrijeme.

Mitts (2005) navodi da je svaki element plana kontinuiteta rada informacionog sistema nužno testirati na neki način, kako bi se implementirana tehnologija pravilno uklopila u cjelokupnu specifikaciju. To je važno jer dokazuje da su planovi za održavanje kontinuiteta rada dobro dokumentovani i izvodivi u realnim kriznim situacijama. Kompanije koje ne testiraju svoje planova za kontinuitet poslovanja ili rada informacionog sistema, ne znaju jesu li sposobne održati proces i pratiti akcije koje plan nalaže, što itekako povećava rizik i dovodi u pitanje samo opstojanje kompanije.

1.1. Predmet i problem istraživanja

Poslovanje u savremenom dobu kompleksno je i dinamično, pa su kompanije uvijek izložene potencijalnim rizicima. Zbog toga se fokusiraju na očuvanje poslovanja kroz primjenu koncepata planiranja kontinuiteta poslovanja, kontinuiranog kompjutinga i oporavka od katastrofa. Postoje razne tehnologije koje omogućavaju implementaciju spomenutih procesa i mehanizama, koje su zapravo ključ uspješnog kontinuiranog poslovanja i kompjutinga. S tim u vezi, u okviru ovog rada bit će izvršena komparativna analiza i pregled IT tehnologija kako bismo stekli bolji uvid u raznolikost alata i sistema.

1.2. Svrha i ciljevi istraživanja

Shodno definisanom predmetu i problemu istraživanja završnog rada, određeni su sljedeći ciljevi:

1. Predstaviti i objasniti osnovne pojmove, procese, elemente i historijat kontinuiteta poslovanja i kontinuiranog kompjutinga;
2. Objasniti koncept i ulogu planiranja i upravljanja kontinuitetom poslovanja;
3. Predstaviti značaj implementacije kontinuiteta poslovanja za kompanije u svrhu upravljanja rizicima i oporavka od katastrofe;
4. Predstaviti značaj implementacije kontinuiteta poslovanja za kompanije u kontekstu upravljanja rizicima;
5. Analizirati, komparirati i predstaviti tehnologije koje se koriste za kontinuirani kompjuting;
6. Predstaviti rezultate komparacije tehnologija za kontinuirani kompjuting.

1.3. Istraživačka pitanja i hipoteze

Istraživačka pitanja na koja će odgovoriti ovaj rad su:

1. Je li implementacija koncepta kontinuiteta poslovanja i kontinuiranog kompjutinga doprinijela poslovanju i sigurnosti kompanija?
2. Je li kontinuirani kompjuting osnova za održiv kontinuitet poslovanja u savremenom dobu?
3. Koje tehnologije za kontinuirani kompjuting se koriste u savremenom poslovnom svijetu?

Uzimajući u obzir ciljeve istraživanja i istraživačka pitanja, formirana je glavna hipoteza:

H1. Implementacija tehnologija za kontinuirani kompjuting ima pozitivan utjecaj na kontinuitet poslovanja kompanija.

Dokazivanje glavne H1 hipoteze će se uraditi kroz kvalitativnu i teoretsku analizu prikupljenih informacija te logičku argumentaciju temeljenu na literaturi, istraživačkim radovima i relevantnim studijama slučaja, citirajući mišljenja stručnjaka iz industrije i njihovih analiza ili praktičnih primjera o implementaciji tehnologija kontinuiranog kompjutinga, kako bismo dobili objektivnu sliku i potvrdili ili opovrgnuli glavnu hipotezu.

Također, dokazivanje glavne H1 hipoteze bit će urađeno pomoću rezultata dvije komparativne analize različitih tehnologija za kontinuirani kompjuting, na osnovu eksploracije prikupljenih relevantnih informacija o prednostima i nedostacima svake tehnologije, koristeći literaturu, stručne izvore i studije slučaja.

Prva komparacija će se zasnivati na upoređivanju tih informacija kako bismo identifikovali zajedničke karakteristike i obrasce koji se pojavljuju među različitim tehnologijama. Naprimjer, uporedit će se performansi, sigurnost, kompleksnost, skalabilnost i fleksibilnost svake tehnologije, identifikujući sličnosti i razlike u tim aspektima.

Druga komparacija će biti predstavljena na osnovu prethodne komparacije, a temeljena je na metodi iz članka „A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability“, koji su napisali M. Al-Kuwaiti, N. Kyriakopoulos i S. Hussein.

1.4. Metodologija istraživanja

U svrhu teorijske analize i izrade završnog rada, bit će korišteni izvori literature kao što su knjige, stručni časopisi i naučni radovi u pisanoj ili online formi, a izvor su i verifikovane internet-stranice.

Na osnovu navedenih izvora literature, uradit će se komparativne analize tehnologija za kontinuirani kompjuting, pri čemu će se izdvojiti osnovne karakteristike svake tehnologije, a upoređivanjem tehnologija, specifikacija i njihovih karakteristika, doći će se do zaključka koja tehnologija ima prednosti ili nedostatke u odnosu na druge. Rezultati će biti prikazani tabelarno ili grafički, ovisno o karakteristikama koje se upoređuju.

Dokazivanje hipoteze bit će urađeno kroz kvalitativnu i teoretsku analizu prikupljenih informacija, temeljenu na literaturi, istraživačkim radovima, relevantnim studijama slučaja, citirajući mišljenja stručnjaka iz industrije i njihovih analiza ili praktičnih primjera o implementaciji tehnologija kontinuiranog kompjutinga. Također, dokazivanje hipoteze bit će urađeno pomoću rezultata komparativnih analiza različitih tehnologija za kontinuirani kompjuting, a na osnovu eksploracije prikupljenih informacija o prednostima i nedostacima svake tehnologije, koristeći literaturu, stručne izvore i studije slučaja.

1.5. Struktura rada

U uvodnom dijelu dati su problem i obrazloženje teme, predmet i problem istraživanja, svrha i ciljevi istraživanja, metodologija istraživanja te struktura rada.

U drugom dijelu rada prezentovani su pregled naučne literature o kontinuitetu poslovanja i kontinuiranom kompjutingu, historijski osvrt i razvoj, upravljanje i planiranje kontinuitetom poslovanja, oporavak od katastrofe i upravljanje rizicima u poslovanju.

U trećem dijelu rada su predstavljeni komparativna analiza tehnologija u kontinuitetu poslovanja, server-računari, operativni sistemi i softveri, baze podataka i tehnologije za *backup* podataka, računarske mreže, *cyber*-sigurnost, *cloud* i virtualizacija, te ostale nove tehnologije. Također je predstavljena komparativna analiza pet ključnih koncepata tehnologija za kontinuirani kompjuting.

U četvrtom dijelu je zaključak u kojem su sumirani i navedeni najvažniji rezultati komparativne analize.

2. KONTINUITET POSLOVANJA I KONTINUIRANI KOMPJUTING

U narednim poglavljima rada bit će objašnjene osnove kontinuiteta poslovanja i kontinuiranog kompjutinga. Također će biti predstavljen historijski razvoj, planiranje i upravljanje kontinuitetom poslovanja te oporavak od katastrofa i rizika.

2.1. Pojmovi kontinuitet poslovanja i kontinuirani kompjuting

Kontinuitet poslovanja (engl. *Business continuity*) predstavlja sposobnost neke organizacije da nastavi sa svojim redovnim poslovima u slučaju pojave nepredviđenih okolnosti, izazova ili incidenata, poput prirodne katastrofe, tehničkog kvara, terorističkog napada ili pandemije. Ovo je bitno za sve organizacije jer im omogućava da se suoče s različitim izazovima i nastave sa svojim poslovnim procesima bez prekida (Hiles, 2007).

Kontinuitet poslovanja je posebno bitan za organizacije koje pružaju usluge ili proizvode, kao što su medicinske ustanove, banke, telekomunikacijske kompanije i ostale za život važne ustanove. Ove organizacije su od ključnog značaja za funkcionisanje društva i ekonomije, pa je važno da nastave sa svojim poslovima, čak i u slučaju pojave nekih izazova (Snedaker, 2007).

Postoje različiti načini na koje organizacije mogu unaprijediti svoj kontinuitet poslovanja. To može uključivati stvaranje planova za krizne situacije, kao što su planovi za evakuaciju, planovi za obnavljanje poslova nakon neke katastrofe i planovi za komunikaciju s javnošću u slučaju incidenata. Planovi za evakuaciju obično se koriste u slučaju požara ili neke druge opasnosti za zdravlje i sigurnost ljudi u zgradi ili prostoru u kojem se nalazi organizacija.

Planovi za obnavljanje poslova koriste se za oporavak organizacije nakon nekog događaja koji je ugrozio njen rad, kao što su potres, požar ili poplava. Planovi za komunikaciju s javnošću koriste se za informisanje javnosti o tome šta se dešava i kako se organizacija suočava s određenim izazovom (Phillips, Landahl, 2020).

Međutim, to nije sve. Kontinuitet poslovanja podrazumijeva i sposobnost organizacije da se brzo adaptira na promjene i nove okolnosti. To zahtijeva da organizacije imaju fleksibilne procese i budu spremne da se prilagode novim situacijama kako bi mogle nastaviti sa svojim poslovima. Pored toga, važno je da organizacije imaju odgovarajuće ljudske i finansijske resurse da bi se mogle suočiti s izazovima i nastaviti sa svojim poslovima (Rezaei *et al*., 2018).

Organizacije mogu unaprijediti svoju sposobnost da se suoče s katastrofama tako što će razviti alternativne kanale komunikacije ili investirati u tehnologije i alate koji će im pomoći da nastave sa svojim poslovima u slučaju prekida, što zapravo i predstavlja kontinuirani kompjuting (Drewitt, 2012).

Kontinuirani kompjuting i kontinuitet poslovanja su povezani pojmovi, oba se odnose na sposobnost organizacija da nastave sa svojim poslovima u slučaju pojave izazova ili prekida. Međutim, postoji određena razlika između ovih pojmova. Kontinuirani kompjuting i kontinuitet poslovanja odnose se na dva različita aspekta rada organizacija.

Kontinuirani kompjuting (engl. *Continuous computing*) jeste tehnologija koja osigurava kontinuirano izvođenje računarskih zadataka u stvarnom vremenu, bez prekida ili zastoja. Ovo se može postići korištenjem specijaliziranog hardvera i softvera dizajniranog za kontinuirano izvršavanje zadataka i procesa ili korištenjem tehnika kao što su grupna obrada (engl. *batch processing*) i obrada u stvarnom vremenu (engl. *real-time processing*). Dakle, fokus je na samoj tehnologiji i njenoj implementaciji u odnosu na kontinuitet poslovanja, gdje je u fokusu sposobnost same organizacije da nastavi sa svojim poslovima u slučaju pojave izazova ili prekida rada (Bajgorić, 2008).

Kontinuirani kompjuting podrazumijeva da implementirana tehnologija u organizaciji ima rezervne sisteme i procese koji se aktiviraju u slučaju prekida rada glavnog sistema, što stvara uvjete za nastavak rada bez prekida. Kontinuirani kompjuting se često koristi u kontekstu *cloud computing* tehnologije, gdje se podaci i aplikacije pohranjuju u „oblaku“ (engl. *cloud*) i omogućavaju pristup s bilo kojeg mjesta, što osigurava organizacijama da nastave s radom, čak i u slučaju prekida u radu glavne lokacije (Bajgorić, 2009).

Ovo može biti od ključnog značaja za organizacije koje se suočavaju s otežanim pristupom svojim podacima ili aplikacijama u slučaju prirodne katastrofe, tehničkog kvara, napada hakera ili druge vrste katastrofa. Bitno je napomenuti da je važno imati stručno osoblje koje je osposobljeno za rukovođenje i upravljanje kontinuiranim kompjutingom, te dobro održavati i nadzirati sisteme i tehnologije koje se koriste u kontinuiranom kompjutingu (Elliott *et al*., 2010).

Posljednjih godina, kontinuirani kompjuting postaje sve važniji jer se sve više kompanija i organizacija oslanja na kompjuterske sisteme za vođenje svojih operacija. Kontinuirani kompjuting omogućava ovim sistemima da rade bez greške i efikasno, te osigurava da se važni poslovni procesi završe na vrijeme, kao što su analiza podataka, finansijske transakcije, proizvodni procesi i naučne simulacije, što može biti kritično za ispunjavanje rokova i održavanje zadovoljstva klijenata (Hiles, 2014).

Oblast kontinuiranog kompjutinga je aktivna oblast istraživanja i razvoja, jer tehnologija napreduje, a pojavljuju se i nove aplikacije za kontinuirani kompjuting. Istraživači i inžinjeri neprestano rade na poboljšanju performansi, pouzdanosti i efikasnosti sistema koji koriste ove tehnologije, s ciljem da kompanije i organizacije u potpunosti iskoriste mogućnosti modernih računarskih sistema. Dakle, kontinuirani kompjuting je suštinski aspekt modernog svijeta i nastavit će igrati vitalnu ulogu u budućnosti kako tehnologija bude napredovala (Kersten, Klett, 2017).

Kontinuirani kompjuting se može koristiti za različite namjene u kontekstu kontinuiranog poslovanja, uključujući (Hiles, 2007):

Automatizaciju poslovnih procesa: Kontinuirani kompjuting omogućava stvaranje autonomnih sistema i automatizaciju poslovnih procesa kao što su obračunavanje plaća, izvještavanje o prodaji i upravljanje inventarom ili proizvodnim linijama. Rezultat je brže i tačnije obavljanje poslova, a također se smanjuje mogućnost grešaka i potreba za ljudskim intervencijama.

Nadgledanje rada: Kontinuirani kompjuting se može koristiti u svrhu nadgledanja rada u stvarnom vremenu te automatskog reagovanja na određene događaje ili promjene. Naprimjer, sistem za nadgledanje rada može automatski izvršiti restart mašine u slučaju da se otkrije neispravnost, čime bi se izbjegao prekid rada, a održao kontinuitet poslovanja.

Real-time računanje**:** Kontinuirani kompjuting se također može koristiti pri automatskoj obradi i analizi velike količine podataka u stvarnom vremenu. Tako se brže donose odluke i poduzimaju odgovarajuće akcije. Naprimjer, sistem za analizu podataka može se koristiti u svrhu analize prodaje kako bi se identifikovali trendovi u finansijskim transakcijama ili ponašanju potrošača, što bi utjecalo na prilagođavanje strategije marketinga i povećanje efikasnosti poslovanja.

2.2. Historijski osvrt i razvoj kontinuiteta poslovanja i kontinuiranog kompjutinga

Koncept kontinuiteta poslovanja seže u davna vremena, kada su se organizacije suočavale s različitim vrstama prijetnji i izazova. Prve implementacije kontinuiteta poslovanja su se, stoga, odnosile na stvaranje rezervnih resursa i sistema koji su omogućavali organizacijama da nastave s radom u slučaju pojave izazova ili kriza. Teško je navesti tačan datum kada je prvi put implementiran plan za kontinuitet poslovanja, jer se ovaj koncept razvijao postepeno kroz historiju (Snedaker, 2007).

Jedan od prvih primjera implementacije kontinuiteta poslovanja mogao bi biti stvaranje rezervnih zaliha hrane i vode, koje su organizacije koristile da bi preživjele u slučaju kriza. Drugi primjer bi bio razvoj planova za evakuaciju i skloništa u slučaju prirodnih katastrofa, kao što su poplave, zemljotresi ili cunamiji (Elliott *et al*., 2010).

Međutim, s razvojem tehnologije, globalizacijom i povećanjem složenosti poslovanja, kontinuitet poslovanja je postao sve složeniji i zahtijeva više od samih fizičkih resursa. U modernom dobu, kontinuitet poslovanja je postao važan i zbog sve veće zavisnosti organizacija od informacionih tehnologija i društvenih mreža. To je dovelo do potrebe za razvijanjem planova za kontinuitet poslovanja, koji uključuju i mjere zaštite od *cyber* napada, pada sistema ili drugih vrsta tehničkih kvarova (Phillips, Landahl, 2020).

U 21. stoljeću se, također, pojavila potreba za razvijanjem fleksibilnijih planova za kontinuitet poslovanja, koji se mogu prilagoditi različitim vrstama izazova i kriza poput klimatskih promjena i pandemija. To je dovelo do razvoja koncepta „agilnog kontinuiteta poslovanja", koji se odnosi na sposobnost organizacije da brzo reaguje i prilagodi se promjenama u okruženju (Applegate *et al*., 2009).

U skladu s razvojem koncepta kontinuiteta poslovanja, pojavili su se različiti standardi i regulative koje nalažu organizacijama da razviju planove za kontinuitet poslovanja, te da ih redovno testiraju i ažuriraju. Ovi standardi uključuju *Business Continuity Institute* (BCI) standard i ISO 22301 standard za kontinuitet poslovanja (Hiles, 2014).

Značajni datumi u historiji kontinuiranog planiranja (Herbane, 2010):

- 1920: Koncept poslovnog planiranja razvio je konsultant za upravljanje Peter Drucker;
- 1950: Termin „kontinuirano planiranje" definisao je konsultant za menadžment Alfred D. Chandler Jr., koji naglašava važnost kontinuiranog pregleda i prilagođavanja poslovnih planova kao odgovor na promjenjive tržišne uvjete;
- 1960: Reinžinjering poslovnih procesa, metoda poboljšanja efikasnosti i efektivnosti kroz redizajn poslovnih procesa, postaje popularan;
- 1990: Koncept agilnog upravljanja projektima, koji uključuje kontinuirano planiranje i ponavljanje, postaje popularan u industriji razvoja softvera;
- 2000: Upotreba alata poslovne inteligencije, koji rade analizu podataka u stvarnom vremenu, postaje široko rasprostranjena, omogućavajući preduzećima da kontinuirano prate i prilagođavaju svoje planove i strategije;
- 2010: Koncept kontinuiranog planiranja postaje sve raširenji kako kompanije usvajaju agilne metodologije i usvajaju digitalne alate koji osiguravaju analizu podataka i donošenje odluka u stvarnom vremenu.

Koncept kontinuiranog kompjutinga ima dugu historiju koja se može pratiti još od ranih dana računarstva. Početkom 20. stoljeća, naučnici i injžinjeri razvili su prve mehaničke i elektromehaničke računare koji su korišteni za obavljanje različitih zadataka, uključujući

naučne proračune, razbijanje kodova i obradu podataka. Ovi rani računari su bili veliki, skupi i teški za upotrebu, i za njihovo pokretanje je bio potreban tim obučenih operatera (Herbane, 2010).

Kroz vrijeme, razvijale su se razne tehnologije za kontinuirani kompjuting, a temelj su postavile sljedeće (Applegate *et al*., 2003; Hiles, 2014):

- Grupna obrada (engl. *batch processing*) jedan je od najranijih oblika kontinuiranog kompjutinga, koji podrazumijeva izvođenje niza zadataka ili procesa u seriji ili grupi, a ne pojedinačno. Dakle, više zadataka se procesuira odjednom, poboljšavajući efikasnost i smanjujući količinu vremena potrebnog za dovršetak zadataka.
- Obrada u stvarnom vremenu (engl. *Real-time processing*), koja podrazumijeva obradu podataka u momentu kada se oni zaprime, dakle trenutno, a ne u serijama. Obrada u stvarnom vremenu se koristi u raznim aplikacijama, uključujući finansijske transakcije, sisteme kontrole saobraćaja, vojne i kontrolne sisteme.
- Distribuisano računarstvo (engl. *distributed computing*). U distribuisanom računarstvu, zadaci ili procesi se distribuišu na više računara ili uređaja, umjesto da se izvode na jednoj mašini. Rezultat je brža obrada i povećana pouzdanost, jer je radno opterećenje raspoređeno na više sistema.
- Računarstvo u „oblaku“ (engl. *cloud computing*) odnosi se na upotrebu udaljenih servera i skladišta za pokretanje i izvršavanje aplikacija i usluga, umjesto njihovog pokretanja na lokalnom hardveru. *Cloud computing* povećava skalabilnost, fleksibilnost i uštedu troškova, jer se resursi mogu dodati ili ukloniti po potrebi.
- „Internet stvari“ (engl. *Internet of Things – IoT*) odnosi se na rastuću mrežu povezanih uređaja koji su u stanju komunicirati jedni s drugima, a i s centralnim serverima. Ovi uređaji se mogu koristiti za prikupljanje i obradu podataka u stvarnom vremenu, omogućavajući kontinuirano praćenje i kontrolu različitih sistema i procesa.

Značajni datumi u historiji implementacije kontinuiranog kompjutinga u kontekstu kontinuiranog planiranja (Herbane, 2010, Hiles, 2014):

- 1960: Elektronski računari počinju se široko koristiti u poslovanju, što ima za posljedicu efikasniju obradu i analizu podataka.
- 1970: Upotreba kompjuterski potpomognutog dizajna (CAD) i proizvodnih (CAM) sistema postaje široko rasprostranjena, povećavajući preduzećima efikasnost dizajniranja i proizvodnje. Zatim, razvoj ekspertnih sistema i sistema za podršku u odlučivanju (DSS), koji su se koristili za donošenje odluka, rješavanje problema, automatizovanje procesa itd.
- 1980: Kompanije počinju usvajati kompjuterski potpomognuto planiranje (CAPS) koje predstavlja sistem za efikasno i efektivno planiranje i raspoređivanje resursa. Zatim, razvoj sistema za planiranje resursa preduzeća (ERP), koji mogu integrisati i upravljati različitim poslovnim procesima, uključujući finansijsko planiranje,

proizvodnju i upravljanje lancem snabdijevanja. Također, razvoj geografskih informacionih sistema (GIS) koji su se koristili za analiziranje i vizualizaciju geografskih podataka u stvarnom vremenu, poboljšavajući donošenje odluka i planiranje.

- 1990: Široko usvajanje personalnih računara (PC) i razvoj softvera za proračunske tablice i baze podataka, što je omogućilo preduzećima da izvode složenije analize i donose odluke na osnovu novih informacija. Zatim, razvoj sistema za upravljanje odnosima s klijentima (CRM), pomoću kojeg su kompanije upravljale podacima o klijentima u stvarnom vremenu i analizirale ih, što je imalo za rezultat efikasnije marketinške i prodajne strategije.
- 2000: Upotreba alata za poslovnu inteligenciju i analizu podataka postaje široko rasprostranjena, tim alatima su preduzeća kontinuirano pratila i analizirala podatke u stvarnom vremenu. Zatim, razvoj sistema upravljanja lancem snabdijevanja, kojim su preduzeća optimizirala protok materijala i proizvoda kroz lanac snabdijevanja, poboljšavajući efikasnost i održivost.
- 2005: Razvoj alata za rudarenje podataka i prediktivne analitike, kojim su se analizirale velike količine podataka i donosile bolje informisane odluke.
- 2010: *Cloud computing* i *Internet of Things* (IoT) osigurava preduzećima da prikupljaju i analiziraju podatke iz širokog spektra izvora, što je pomoglo pri efikasnijem kontinuiranom planiranju. Zatim, usvajanje agilnih metodologija upravljanja projektima, koje uključuju kontinuirano ponavljanje i planiranje, postaje široko rasprostranjeno u industriji razvoja softvera.

2.3. Upravljanje kontinuitetom poslovanja i planiranje

Upravljanje kontinuitetom poslovanja (BCM) i kontinuitet poslovanja su pojmovi koji se često koriste u kontekstu osiguravanja nastavka rada organizacije u slučaju nekih neplaniranih događaja ili incidenata. Međutim, postoji razlika između ovih pojmova.

Upravljanje kontinuitetom poslovanja (engl. *Business Continuity Management, BCM*) jeste proces koji se odnosi na planiranje, organizaciju i implementaciju mjera za osiguravanje nastavka rada organizacije u slučaju pojave nekih neplaniranih događaja ili incidenata koji bi mogli ugroziti njen rad. BCM je proces koji se odnosi na cijelu organizaciju i uključuje sve aspekte poslovanja, od proizvodnje do isporuke proizvoda ili usluga klijentima (Phillips, Landahl, 2020).

Kontinuitet poslovanja je stanje u kojem organizacija nastavlja rad u što normalnijim okolnostima, čak i u slučaju pojave nekih neplaniranih događaja ili incidenata. Kontinuitet poslovanja je cilj BCM-a, a postiže se kroz implementaciju mjera za osiguravanje nastavka rada organizacije (Hiles, 2014).

Ukratko, razlika između upravljanja kontinuitetom poslovanja (BCM) i kontinuiteta poslovanja je u tome što BCM predstavlja proces koji se odnosi na planiranje i

implementaciju mjera za osiguravanje nastavka rada organizacije, dok kontinuitet poslovanja predstavlja stanje u kojem organizacija nastavlja rad u što normalnijim okolnostima.

Upravljanje kontinuitetom poslovanja je bitno za sve organizacije jer im omogućava da se prilagode promjenama u okruženju i osiguraju nastavak poslovanja u slučaju nekih neplaniranih događaja ili incidenata. To znači da će organizacija biti u stanju nastaviti isporučivati proizvode ili usluge svojim klijentima, te da će biti u stanju nastaviti izvršavati svoje obaveze prema drugim saradnicima, poput zaposlenika ili vendora. To je važno za očuvanje ugleda organizacije i zadovoljstva klijenata i drugih sudionika u procesu poslovanja. Ako organizacija nema plan za upravljanje kontinuitetom poslovanja, postoji veliki rizik da će se njen rad zaustaviti ili otežati u slučaju pojave takvih događaja ili incidenata, što može dovesti do finansijskih gubitaka i oštećenja reputacije. BCM se može primijeniti u različitim granama industrije, kao što su bankarski i finansijski sistemi, telekomunikacije, uslužne i proizvodne djelatnosti. U svakoj grani industrije, BCM se prilagođava specifičnostima organizacije i okruženja u kojem se vrši proces poslovanja. (Elliott *et al*., 2010).

Neke od značajnih karakteristika upravljanja kontinuitetom poslovanja (Snedaker, 2007) jesu:

- Holistički pristup: odnosi se na cijelu organizaciju i uključuje sve aspekte poslovanja, od proizvodnje do isporuke proizvoda ili usluga klijentima.
- Integrisano: inkorporiran je u sve aspekte poslovanja organizacije i ne treba ga posmatrati kao odvojenu aktivnost.
- Proaktivan: bazira se na proaktivnom pristupu, što znači da organizacija unaprijed planira i sprema se za moguće rizike i incidente, umjesto da reaguje na njih kada se već dogode.
- Cikličan: proces kontinuiteta poslovanja se planira ciklično i sastoji se od nekoliko faza. Od definisanja ciljeva i kritičnih funkcija, preko analize rizika i planiranja, do implementacije i testiranja plana.
- Dokumentiran: upravljanje kontinuitetom poslovanja se temelji na dokumentaciji, što znači da se sve mjere i postupci moraju detaljno opisati i dokumentovati.
- Redovno revidiran: ovaj način upravljanja treba redovno revidirati i ažurirati, kako bi se osiguralo da je plan za upravljanje kontinuitetom poslovanja u skladu s promjenama u okruženju i potrebama organizacije.
- Saradnja: temelji se na saradnji između različitih dijelova organizacije i može uključivati saradnju s vanjskim partnerima, poput vendora i državnih tijela.

Upravljanje kontinuitetom poslovanja (BCM) danas se koristi u različitim organizacijama širom svijeta, bilo da se radi o malim porodičnim kompanijama ili velikim korporacijama. U modernim organizacijama, BCM se koristi kako bi se osiguralo da se rad organizacije

nastavi u što normalnijim okolnostima, čak i u slučaju pojave nekih neplaniranih događaja ili incidenata. BCM se može koristiti za različite svrhe (Drewitt, 2012), uključujući:

- Osiguranje da se rad organizacije nastavi u što normalnijim okolnostima, čak i u slučaju pojave nekih neplaniranih događaja ili incidenata;
- Smanjenje vremena obnove poslovanja nakon incidenta;
- Smanjenje šteta koje bi incident mogao uzrokovati;
- Očuvanje ugleda organizacije i zadovoljstva klijenata;
- Osiguranje da se organizacija može prilagoditi promjenama u okruženju.

Planiranje kontinuiteta poslovanja (BCP) i upravljanje kontinuitetom poslovanja (BCM) pojmovi su koji se često koriste u kontekstu osiguravanja nastavka rada organizacije, međutim, postoji koncizna razlika između ovih pojmova.

Planiranje kontinuiteta poslovanja (BCP) dio je upravljanja kontinuitetom poslovanja (BCM) koji se odnosi na definisanje i planiranje mjera koje će organizacija poduzeti kako bi osigurala nastavak rada u slučaju pojave nekih neplaniranih događaja ili incidenata. Upravljanje kontinuitetom poslovanja (BCM) širi je proces koji se odnosi na planiranje, organizaciju i implementaciju mjera za osiguravanje nastavka rada organizacije u slučaju pojave nekih neplaniranih događaja ili incidenata koji bi mogli ugroziti njen rad.

Ukratko, razlika između planiranja kontinuiteta poslovanja (BCP) i upravljanja kontinuitetom poslovanja (BCM) jeste u tome što BCP predstavlja dio BCM-a koji se odnosi na definisanje i planiranje mjera za osiguravanje nastavka rada organizacije, dok BCM predstavlja širi proces koji se odnosi na planiranje, organizaciju i implementaciju mjera za osiguravanje nastavka rada organizacije u cjelini (Phillips, Landahl, 2020).

Razvoj planiranja kontinuiteta poslovanja (BCP) jeste proces koji se odvija tokom vremena i koji uključuje nekoliko koraka (Lam, 2002):

- Identifikacija kritičnih funkcija: Prvi korak u BCP-u je identifikacija kritičnih funkcija organizacije, odnosno dijelova poslovanja koji su ključni za njen rad i čiji nastavak bi se trebalo osigurati u slučaju pojave nekih neplaniranih događaja ili incidenata.
- Analiza rizika: Nakon identifikacije kritičnih funkcija, slijedi analiza rizika koji bi mogli ugroziti rad organizacije i utvrđivanje vjerovatnosti rizika, te posljedica pojave takvih rizika. Analiza rizika je važan korak u razvoju BCP-a, jer ona prepoznaje prioritete i ukupni impakt rizika na organizaciju.
- Planiranje: Treći korak je planiranje mjera za osiguravanje nastavka rada organizacije u slučaju pojave rizika. To uključuje definisanje plana za obnovu poslovanja nakon incidenta, odnosno plana za povratak na normalno stanje rada. Planiranje BCP-a obično uključuje izradu detaljnih uputa i postupaka za svaku kritičnu funkciju, kao i definisanje odgovornosti i uloga osoblja u slučaju pojave incidenta.

- Implementacija: Četvrti korak je implementacija plana za BCP, što uključuje stvaranje tima za upravljanje kontinuitetom poslovanja, pripremu potrebnih resursa i alata, te obučavanje osoblja o postupcima i mjerama koje treba poduzeti u slučaju pojave incidenta.
- Testiranje i revidiranje: Posljednji korak u razvoju BCP-a je testiranje i revidiranje plana za BCP, kako bi se osiguralo da je plan učinkovit i da odgovara promjenama u okruženju i potrebama organizacije. Testiranje BCP-a obično uključuje simulacije i vježbe kojima se provjerava sposobnost organizacije da nastavi rad u slučaju pojave incidenta, te utvrđivanje mogućih nedostataka u planu i potrebne izmjene.

Za planiranje kontinuiteta poslovanja i njegovo upravljanje veoma su bitne IT tehnologije jer omogućavaju organizacijama da se brže i efikasnije nose s pojavom nekih neplaniranih događaja ili incidenata te da nastave rad u što normalnijim okolnostima. IT tehnologije imaju nekoliko ključnih uloga u upravljanju kontinuitetom poslovanja i njegovom planiranju (Bowman, 2008):

- Poboljšanje raspoloživosti: IT tehnologije osiguravaju organizacijama da poboljšaju raspoloživost svojih IT resursa i nastave rad u što normalnijim okolnostima, čak i u slučaju pojave nekih neplaniranih događaja ili incidenata.
- Brže reagovanje: koristeći IT tehnologije, organizacije brže reaguju na pojavu nekih neplaniranih događaja ili incidenata, te poduzimaju odgovarajuće mjere za osiguravanje nastavka rada.
- Lakše prilagođavanje: s IT tehnologijama organizacije se lakše prilagođavaju promjenama u okruženju te nastavljaju s radom u što normalnijim okolnostima.
- Poboljšanje sigurnosti: IT tehnologije pomažu organizacijama da poboljšaju sigurnost svojih IT resursa te sprečavaju ili smanjuju utjecaj nekih neplaniranih događaja ili incidenta na rad organizacije.
- Poboljšanje komunikacije: IT tehnologije stvaraju uvjete da organizacije poboljšaju komunikaciju unutar i izvan organizacije, što im pomaže da brže reaguju na pojavu nekih neplaniranih događaja ili incidenata te da nastave rad u što normalnijim okolnostima.

O važnosti planiranja kontinuiteta poslovanja govori Cerullo (2004), gdje u svom radu navodi kako je istraživanje Federalne agencije za vanredne situacije (FEMA) pokazalo da je između 1976. i 2001. zabilježeno ukupno 906 katastrofa u Sjedinjenim Državama. Desetine hiljada organizacija svih veličina su bile pogođene ovim katastrofama. Ako firme nisu unaprijed spremne, katastrofe će zasigurno zaustaviti njihovo poslovanje. Što je duže poslovanje firme zaustavljeno, time raste vjerovatnoća da nikada više neće nastaviti s radom.

U studiji koju ja uradila kompanija „Datapro Research“, navedeno je da 43 posto kompanija pogođenih teškim krizama nikada ne nastavi normalno poslovanje, a 29 posto propadne u roku od dvije godine nakon nastavljanja rada. Prema FEMA-i, od svih preduzeća oštećenih

uraganom Andrew 1992. godine, 80 posto onih organizacija koje nemaju plan kontinuiteta poslovanja (BCP), dvije godine od oluje prestalo je s radom.

2.4. Oporavak od katastrofe

Oporavak od katastrofe se odnosi na planove i mjere koje organizacije razvijaju da bi se suočile s posljedicama elementarnih nepogoda, tehničkih kvarova ili *cyber* napada. U sklopu ovih planova, organizacije obično razvijaju mjere za vraćanje u rad računarskih sistema i drugih važnih resursa, te mjere za komunikaciju sa zaposlenima i drugim važnim sudionicima poslovanja u slučaju pojave katastrofe (Engemann, Henderson 2011).

U toku 21. stoljeća, oporavak od katastrofe se nastavio razvijati u skladu s razvojem tehnologije i povećanjem složenosti poslovanja. U ovom periodu su se pojavile nove vrste izazova za oporavak od katastrofe, poput klimatskih promjena i pandemija, što je dovelo do potrebe za razvijanjem fleksibilnijih planova za oporavak od katastrofe, koji se mogu prilagoditi različitim vrstama izazova i kriza (Whitman, Mattord, 2021).

Implementacija planova za kontinuitet poslovanja i oporavak od katastrofe zahtijeva određena finansijska ulaganja, ali ona su sigurno isplativa u slučaju pojave izazova ili kriza. Organizacije koje razviju i održavaju dobre planove za kontinuitet poslovanja i oporavak od katastrofe su sposobnije da se suoče s izazovima i nastave s radom, što im omogućava da izbjegnu gubitke i održe svoju reputaciju (Mitts, 2005).

Da bi razvile dobre planove za kontinuitet poslovanja i oporavak od katastrofe, organizacije trebaju raditi na identifikaciji i analizi mogućih izazova i rizika. Ovo uključuje procjenu potencijalnih kvarova ili drugih problema s računarskim sistemima i drugim važnim resursima, te identifikaciju mogućih scenarija za suočavanje s ovim izazovima.

Organizacije također trebaju razviti mjere za vraćanje u rad računarskih sistema i drugih važnih resursa u slučaju pojave katastrofe, kao i mjere za komunikaciju sa zaposlenima i drugim važnim segmentima poslovanja u ovom slučaju. Ovi planovi trebaju biti prilagođeni specifičnim potrebama i okruženju organizacije (Speight, 2011).

Lewis (2005) u svom članku navodi da, prema podacima studije iz 2004. godine, koju su objavili „Deloitte & Touche LLP“ i „CPM Global Assurance“, samo oko 50 posto kompanija je implementiralo, na nivou cijele kompanije, planove oporavka od katastrofe i planove kontinuiteta poslovanja.

Prema studiji „AT&T“ i „Partnership“ iz 2004. godine, devetnaest od stotinu kompanija je pretrpjelo katastrofu koja je dovela do toga da njihova organizacija prestane s radom na određeni vremenski period.

2.5. Upravljanje rizicima u poslovanju

Upravljanje rizicima u poslovanju je važna aktivnost koja se odnosi na identifikaciju, procjenu i kontrolu mogućih izazova i rizika s kojima se organizacija može suočiti. Ovaj proces se odvija u cilju smanjenja potencijalnih negativnih posljedica i osiguranja uspješnosti poslovanja (Engemann, Henderson, 2011).

Identifikacija rizika je prvi korak u upravljanju rizicima. Ova aktivnost podrazumijeva identifikaciju svih mogućih izazova i rizika s kojima se organizacija može suočiti, bilo da su interni ili eksterni. Interni rizici su oni koji dolaze iz unutrašnjih procesa organizacije, dok su eksterni rizici oni koji dolaze iz vanjskog okruženja.

Nakon što se rizici identifikuju, potrebno ih je procijeniti. Ova aktivnost podrazumijeva procjenu vjerovatnosti da se rizik dogodi i ocjenu posljedica koje bi se dogodile u slučaju da se rizik realizuje. Ove ocjene pomažu organizaciji da odluči koliko je važno upravljati određenim rizikom i koje mjere treba poduzeti da bi se rizik smanjio.

Kontrola rizika je posljednji korak u upravljanju rizicima. Podrazumijeva implementaciju mjera za smanjenje vjerovatnosti da se rizik dogodi i smanjenje posljedica koje bi se dogodile u slučaju da se rizik realizuje. Mjere za kontrolu rizika mogu uključivati prevenciju, mitigaciju, transferiranje ili prihvaćanje rizika (Hubbard, 2020).

Upravljanje rizicima pomaže organizaciji da se suoči s izazovima te održi svoju reputaciju i izbjegne gubitke u slučaju pojave katastrofa ili kriza. Postoje različiti pristupi upravljanju rizicima, a koji se odabiru ovisno o specifičnim potrebama i ciljevima organizacije. Neki od poznatih pristupa su (Snedaker, 2007):

- Analiza rizika: Ova metoda se odnosi na detaljnu procjenu rizika, uključujući identifikaciju, procjenu vjerovatnosti i posljedica, te odabir mjera za kontrolu rizika.
- Upravljanje rizicima na projektima: Ova metoda se odnosi na upravljanje rizicima u okviru projekata, uključujući identifikaciju, procjenu i kontrolu rizika koji se pojavljuju tokom cijelog životnog ciklusa projekta.
- Upravljanje rizicima u okviru poslovanja: Ova metoda se odnosi na upravljanje rizicima u okviru poslovanja, uključujući identifikaciju, procjenu i kontrolu rizika koji se pojavljuju u svakodnevnom poslovanju organizacije.

Važno je napomenuti da upravljanje rizicima ne garantuje potpunu eliminaciju rizika, već samo smanjenje vjerovatnosti da se rizik dogodi i smanjenje posljedica koje bi se dogodile u slučaju da se rizik realizuje. Upravljanje rizicima se često koristi u kombinaciji s drugim pristupima, kao što su planiranje, kontrola i upravljanje kvalitetom. Ovaj integrisani pristup omogućava organizaciji da se suoči s izazovima i nastavi s radom, te unaprijedi svoje poslovanje i postigne dugoročni uspjeh (Engemann, Henderson 2011).

3. IMPLEMENTACIJE TEHNOLOGIJA ZA KONTINUIRANI KOMPJUTING: KOMPARATIVNA ANALIZA

Kao što je obrazloženo, da bi se osiguralo uspješno implementiranje kontinuiranog kompjutiranja u svrhu kontinuiteta poslovanja, potrebno je imati dobar i detaljan plan za spremanje organizacije u slučaju nepredviđene situacije i incidenta, kao i stalno ažurirati i testirati taj plan. Također je važno imati stručno osoblje koje je osposobljeno za rukovođenje i upravljanje kontinuiranim kompjutingom, te dobro održavati i nadzirati sisteme i tehnologije koji se koriste u kontinuiranom kompjutiranju.

Kontinuirani kompjuting se može implementirati na različite načine, uključujući upotrebu posebnih hardverskih uređaja ili softverskih rješenja kao što su (Hiles 2014, Drewitt 2012, Bajgorić 2008, Snedaker, 2007):

- server-računari i server operativni sistemi,
- baze podataka i tehnologije za *backup* podataka,
- računarske mreže,
- *cyber*-sigurnost,
- *cloud computing* i virtualizacija i
- ostale nove tehnologije.

Neke od ovih tehnologija, same po sebi, nisu tehnologije za kontinuirani kompjuting ili kontinuirano poslovanje, ali mogu doprinijeti sprečavanju katastrofa, povećanju sigurnosti, ubrzati poslovne procese itd. U narednim poglavljima će biti predstavljene tehnologije koje se koriste za kontinuirani kompjuting i njihova komparativna analiza.

Komparativna analiza se veoma često koristi kao metoda analize u naučnim radovima. Ona se zasniva na komparaciji dvije ili više tehnologija, metoda, pristupa ili rješenja. Komparativna analiza se može definisati i kao metoda kojoj je u fokusu upoređivanje sličnih pojava, kako bi se utvrdile njihove sličnosti i razlike (Bajgorić *et al*., 2019)

Jedan od osnovnih ciljeva komparative analize jeste opis funkcije, ponašanja i strukture dviju ili više pojava koje se istražuju. Ovo podrazumijeva (Zelenika, 2020):

1. otkriti zajedničke karakteristike ili različitosti tih stvari ili pojava,
2. izdvojiti ključne osobine tih pojava,
3. pronaći prednosti i nedostatke pojava.

Naspram navedenih stavki, urađena je i komparativna analiza te su rezultati predstavljeni u narednim poglavljima u vidu tabelarnih prikaza prednosti i nedostataka implementacije tehnologija za kontinuirani kompjuting. Na kraju ovog poglavlja su predstavljene ključne osobine ovih tehnologija, kroz komparaciju koncepata kontinuiranog kompjutinga.

3.1. Server-računari

Server-računari koriste se za obradu i pohranu podataka te za pružanje usluga drugim računarima i uređajima. Oni obično imaju veću izdržljivost i performanse od običnih komercijalnih ili personalnih računara, što ih čini pogodnima za obradu velikih količina podataka i pružanje usluga za više korisnika simultano. To se postiže korištenjem više procesora, više RAM-a i boljeg hardvera općenito (Bryhni *et al*., 2000).

Chevance (2005) u svom radu pojašnjava kako su se server-računari počeli koristiti u poslovnom okruženju od 1950-ih, kada su se pojavili prvi veliki računari koji su služili za obradu podataka u korporacijama. S vremenom, server-računari su postali sve sofisticiraniji i sposobni su pružati različite usluge, poput pohrane podataka, elektronske pošte, web-servisa i drugih. Server-računari također imaju sisteme za upravljanje i nadzor rada, kojima administratori održavaju server računara i osiguravaju da rade ispravno. To uključuje mjere poput automatskog restarta u slučaju pogreške, *backupa* podataka za slučaj gubitka podataka i zaštite od virusa i drugih zlonamjernih programa.

Postoje različite vrste server-računara (Held, 2000), uključujući:

- Web-serveri: računari koji služe za hosting web-stranica, a kojima korisnici pristupaju putem interneta.
- Mail-serveri: računari koji služe za razmjenu elektronske pošte.
- File-serveri: računari koji služe za pohranu i dijeljenje datoteka među različitim računarima, uređajima i korisnicima.
- Database-serveri: računari koji služe za pohranu i upravljanje bazama podataka.
- Aplikacijski serveri: računari na kojima se pokreću aplikacije te pružaju usluge drugim računarima i uređajima.

Server-računari kao redundantni uređaji mogu biti način implementacije tehnologije za kontinuirani kompjuting. Kao alat redundancije, serveri imaju bitnu ulogu u osiguravanju neprekidnosti poslovanja, a u tabeli 1 su navedene neke od glavnih prednosti i nedostataka redundancije server-računara:

Tabela 1. Komparacija redudantnih server-računara

Redundantni server-računari	
Prednosti	Nedostaci
- Jednostavnost implementacije: Redundantni serveri su relativno jednostavni za implementaciju i održavanje. Koncept oslanjanja na više fizičkih servera za povećanje dostupnosti je intuitivan i lako razumljiv.	- Troškovi: Implementacija redundantnih servera može biti skupa, pogotovo kada se uzimaju u obzir troškovi hardvera, licenciranja softvera i održavanja. S povećanom količinom hardvera i softvera povećavaju se i operativni troškovi.

- Visoka razina kontrole: Kroz konfiguraciju redundantnih servera, administratori imaju visoku razinu kontrole nad infrastrukturom i mogu prilagoditi postavke prema specifičnim zahtjevima i potrebama organizacije. - Fleksibilnost: Redundantni serveri mogu se prilagoditi različitim potrebama, omogućavajući skaliranje i prilagodbu infrastrukture u skladu s rastom poslovanja. - Visoka pouzdanost: Korištenje redundantnih servera osigurava visoku razinu pouzdanosti, jer u slučaju kvara jednog servera, drugi preuzimaju teret bez gubitka usluge.	- Složenost skaliranja: Dodavanje redundantnih servera ili proširenje postojeće infrastrukture može zahtijevati složeno planiranje i dodatne resurse. - Kritična tačka sistema: Iako su redundantni serveri dizajnirani da minimiziraju rizik od prekida, postoji i rizik od *single point of failure* (SPOF) situacija ako se ne implementiraju pravilno. Problem se ogleda u tome što server ima mnogo osjetljivih komponenti, gdje kvar jedne ima posljedice na ispravno funkcionisanje servera. - Skaliranja: Dodavanje dodatnih redundantnih servera ili proširenje postojeće infrastrukture može biti složeno i zahtijevati značajno planiranje i resurse.

Izvori: Dreibholz, Rathgeb, (2009;, Huang, Arsenault, Sood, (2006); Guo, Yang, (2014); Kwon et al. (2014); Anton, et al. (2019); Venkatakrishnan, (2014); Machida, Kawato, Maeno, (2010); Gardner et al. (2017)

3.2. Server operativni sistemi

Server operativni sistemi su važni za kontinuirano poslovanje jer omogućavaju kompanijama da efikasno upravljaju i održavaju svoje IT infrastrukture. Oni su odgovorni za upravljanje sistemskim resursima kao što su memorija, procesori, diskovi i mreža, te višestruko istovremeno izvršavanje aplikacija i usluga. Kontinuirano poslovanje zahtijeva stabilnost i dostupnost tih sistema. Server operativni sistemi to osiguravaju kroz mehanizme kao što su automatsko održavanje, sigurnosne mjere i alate za monitoring i dijagnostiku. Kontinuirani rad aplikacija i usluga osigurava da poslovanje kompanije ne bude prekinuto ili ometano (Bajgorić, 2009).

Server operativni sistemi su kompjuterski operativni sistemi koji se koriste za upravljanje i održavanje servera. Oni su dizajnirani da podržavaju veći broj korisnika i zahtjeva za resurse u odnosu na operativne sisteme za komercijalne, tj. personalne računare. Postoje različiti tipovi server operativnih sistema, uključujući *Windows Server*, *Linux* i *Unix*. *Windows Server* je operativni sistem koji se koristi u mnogim poslovnim okruženjima i podržava različite aplikacije i usluge, kao što su *Active Directory*, *Exchange* i SQL server. *Linux* i *Unix* su popularni *open-source* operativni sistemi koji se često koriste za web-server i bazu podataka (Turban, Volonino, 2011).

Server operativni sistemi pružaju mnoge korisne funkcije za upravljanje serverima, kao što su automatizacija zadataka, kontrola pristupa, *backup* i *disaster recovery*. Također, podržavaju pristup s udaljenog mjesta, putem kojeg sistemski administratori mogu upravljati i održavati servere iz bilo kojeg mjesta. Međutim, server operativni sistemi mogu potencijalno imati sigurnosne rizike ako se ne konfigurišu i ne održavaju pravilno. To može dovesti do kompromitovanja podataka i mreže. Shodno tome, važno je da administratori imaju visok nivo stručnosti u konfiguraciji i održavanju server operativnih sistema, kao i da se redovno provode sigurnosne provjere (Snedaker, 2007).

Popularnost server operativnih sistema se mijenja kroz vrijeme, te korištenost varira u zavisnosti od lokacije i industrije. U tabeli 2 se nalaze neke od glavnih prednosti i mana ovih server operativnih sistema:

Tabela 2. Komparacija server operativnih sistema

Windows Server	
Prednosti	Nedostaci
- Grafički korisnički interfejs: *Windows Server* nudi grafički korisnički interfejs koji olakšava rad sa serverom i administracijom resursa. - Podrška za aplikacije: *Windows Server* ima veliku bazu aplikacija koje su prilagođene za rad na njemu, što olakšava implementaciju i upravljanje. - *Active Directory*: *Windows Server* ima integrisanu podršku za *Active Directory*, što omogućava centralizovano upravljanje korisničkim računima i permisijama, kao i sigurnosnim pravilima. - *Remote Desktop Services*: *Windows Server* podržava *Remote Desktop Services*, što nudi korisnicima mogućnost da se povežu sa serverom putem *Remote Desktop* protokola kako bi radili na serveru sa svojih lokalnih računara. - Integracija s *Microsoft* ekosistemom: *Windows Server* se dobro integriše s drugim *Microsoft* proizvodima, kao što su	- Visoki troškovi licenciranja: *Windows Server* je komercijalni proizvod koji se prodaje po licenci, što iziskuje velike troškove ako je potrebno više licenci. - Manja sigurnost: *Windows Server* je više izložen ranjivostima zbog svoje popularnosti i široke baze korisnika. To znači da je potrebno redovno ažuriranje verzija sistema da bi se zadržala sigurnost. - Manja fleksibilnost: *Windows Server* ima manju fleksibilnost u poređenju sa nekim „open-source“ sistemima kao što je *Linux,* što se odnosi na modifikaciju koda, prilagođavanje i automatizaciju rada. - Ograničena podrška za virtualizaciju: *Windows Server* podržava *Hyper-V* kao svoju platformu za virtualizaciju, što može ograničiti opcije za organizacije koje koriste druge platforme za virtualizaciju. - Zavisnost od *Microsoft* ekosistema: *Windows Server* je dizajniran da se integrira sa drugim *Microsoft* proizvodima, što znači da organizacije moraju da koriste *Microsoft*

Exchange, SharePoint, i SQL Server, što za rezultat ima bolju podršku i kompatibilnost.	proizvode za optimalan rad, što ograničava opcije za integraciju s drugim sistemima i aplikacijama.
Linux	
Prednosti	Nedostaci
- Besplatan: *Linux* je *open-source* operativni sistem, što znači da ga je moguće besplatno koristiti, modifikovati i distribuisati. - Stabilnost i sigurnost: *Linux* je poznat po svojoj stabilnosti i sigurnosti, što ga čini idealnim izborom za organizacije. - Visoka performansa: *Linux* je također poznat po visokoj performansi, što je ključno za aplikacije koje zahtijevaju visoku propusnost i nisku latenciju. - Veliki broj alata i aplikacija: *Linux* ima pristup velikom broju alata i aplikacija za upravljanje, što administratorima ostavlja prostora da prilagode server prema potrebama svog okruženja. - Fleksibilnost: *Linux* serveri su fleksibilni, tako da korisnici mogu upotrebljavati različite distribucije, konfiguracije i aplikacije, što je ključno za različite poslovne potrebe.	- Podrška: *Linux* ima manju podršku od drugih operativnih sistema, što znači da neke aplikacije i uređaji mogu biti nekompatibilni s *Linuxom*. - Zajednica: *Linux* ima manju zajednicu od drugih operativnih sistema, što znači da može biti teže pronaći pomoć i savjete u slučaju problema. - Poznavanje: *Linux* zahtijeva više tehničkog znanja od drugih operativnih sistema, što znači da administrativni rad može biti teži i kompleksniji. - Kompatibilnost: *Linux* serveri mogu imati problema s kompatibilnošću nekih softverskih rješenja i hardvera koji nije osmišljen za rad s *Linuxom*. - Aplikacije: Linux ima manje aplikacija dostupnih u odnosu na druge operativne sisteme, što može biti problem za organizacije koje koriste specifične aplikacije.
UNIX	
Prednosti	Nedostaci
- Visok nivo kontrole: *UNIX* pruža visok nivo kontrole nad sistemom, što omogućava administratorima da prilagode server prema potrebama svog okruženja. - Stabilnost i sigurnost: *UNIX* je poznat po svojoj stabilnosti i sigurnosti, što ga čini idealnim izborom za server.	- Skupo licenciranje: *UNIX* server operativni sistem je skuplji od drugih server operativnih sistema, što ga čini manje pristupačnim za male i srednje organizacije. - Složenost: *UNIX* server operativni sistem je generalno složeniji za upravljanje i administraciju u odnosu na druge server

- Visoka performansa: *UNIX* serveri su poznati po visokoj performansi, što je ključno za aplikacije koje zahtijevaju visoku propusnost i nisku latenciju. - Fleksibilnost: *UNIX* serveri su fleksibilni i konfigurabilni, tako da administratori imaju široku paletu distribucija, konfiguracija i aplikacija na raspolaganju. - Velika zajednica: *UNIX* ima veliku zajednicu, što znači da je lahko pronaći pomoć i savjete u slučaju problema.	operativne sisteme, što zahtijeva više stručnosti i iskustva od administratora. - Ograničene aplikacije: Broj aplikacija kompatibilnih s *UNIX* operativnim sistemima je manji u odnosu na Windows i Linux operativne sisteme. - Manje podrške za hardver: *UNIX* operativni sistemi manje podržavaju različite vrste hardvera u odnosu na druge server operativne sisteme.

Izvori: Dauti, (2022); Snedaker, (2007); Economides, Katsamakas, (2006); Adekotujo et al. (2020); Altheide, Carvey, (2011); Kernighan, (2019); Awan, Khan, (2022); Smith, (2005); Khan (2020); Turban, Volonino (2011)

3.3. Baze podataka i tehnologije za backup podataka

Baze podataka su sistemi koji se koriste za pohranu, organizaciju i pretraživanje podataka. Oni su neophodni za funkcionisanje mnogih organizacija i industrija, kao što su trgovina, finansije, zdravstvo i državna uprava. Postoje različiti tipovi baza podataka, kao što su relacijske, objektno-relacijske i NoSQL baze podataka. Relacijske baze podataka koriste relacije između tabela kako bi podaci bili konzistentni i lahko dostupni. Objektno-relacijske baze podataka kombinuju koncepte relacijskih i objektno-orijentisanih baza podataka. NoSQL baze podataka se koriste za pohranu velikih količina podataka i mogu se lahko skalirati (Elmasri, Navathe, 2015).

Baze podataka su ključne za poslovni kontinuitet jer omogućavaju pohranu, organizaciju i pristup podacima koji su neophodni za funkcionisanje poslovanja. One su važne za sve faze poslovanja, od planiranja i izvođenja do praćenja i analize rezultata. U slučaju katastrofe, poput prirodnih nezgoda ili tehničkih kvarova, baze podataka mogu biti presudne za nastavak poslovanja. Ako se podaci pohranjuju pomoću nekih od *backup* tehnologija, oni se mogu brzo vratiti i nastaviti poslovanje bez prekida (McNurlin *et al*., 2014).

Backup tehnologije su neophodne za održavanje poslovnog kontinuiteta jer u slučaju katastrofa, kao što su požar, poplave ili krađa, *backup* tehnologije omogućavaju da se podaci vrate i posao nastavi bez prekida. Postoji više tehnologija za *backup* podataka koje se koriste u kombinaciji s bazama podataka (Whitman, Mattord, 2021):

- Sigurnosna kopija podataka: Postoje sigurnosne kopije na traci (engl. *tape drive*), na disku (engl. *disk-based*) i *cloud backup*. *Tape drive* se koristi za pohranu podataka

na trajne medije kao što je traka. *Disk-based backup* koristi hard-disk za pohranu podataka. *Cloud backup* osigurava pohranu podataka na *cloud s*erverima.

- Inkrementalni (engl. *incremental*) ili diferencijalni (engl. *differential) backup*: Inkrementalni *backup* pohranjuje samo nove i izmijenjene podatke dok diferencijalni *backup* pohranjuje sve promjene od posljednjeg punog *backupa*.
- *Mirroring*: Tehnologija koja kopira podatke u stvarnom vremenu na drugi disk ili server. Ako jedan disk postane neupotrebljiv, drugi disk preuzima njegovu funkciju i osigurava nastavak poslovanja.
- RAID (*Redundant Array of Independent Disks*) jeste tehnologija koja koristi više diskova za pohranu podataka. RAID se koristi za pohranu podataka na serverima, radnim stanicama i drugim uređajima.
- Replikacija podataka je proces kopiranja podataka s jednog mjesta na drugo, što znači da su podaci pohranjeni na više mjesta, a koriste se kao jedna cjelina. RAID ima slične prednosti i nedostatke kao i replikacija podataka, međutim, RAID se fokusira na sigurnost i performanse na nivou hardvera, dok replikacija podataka koristi softverska rješenja.

Svaka od ovih tehnologija ima svoje prednosti i nedostatke, ali svaka od njih ima za cilj osigurati nastavak poslovanja u slučaju gubitka podataka. U tabeli 3 se nalaze prednosti i nedostaci:

Tabela 3. Komparacija backup tehnologija

Sigurnosna kopija baze podataka: Tape drive	
Prednosti	Nedostaci
- Velik kapacitet: Trake su sposobne pohraniti velike količine podataka, što omogućava kreiranje kopija velikih sistema i podataka. - Niska cijena: Trake su relativno jeftine u odnosu na druge medije za pohranu podataka. - Pouzdanost: Trake su otporne na fizička oštećenja i mogu se koristiti za dugoročnu pohranu podataka.	- Ograničena brzina: Proces kreiranja i vraćanja sigurnosnih kopija s trake je sporiji u odnosu na druge medije. - Ovisnost o uređaju: Potreban je poseban uređaj za čitanje trake, što otežava pristup podacima u slučaju kvara uređaja.
Sigurnosna kopija baze podataka: Disk drive	
Prednosti	Nedostaci
- Brzina: Proces kreiranja i vraćanja sigurnosnih kopija s *disk drivea* je brži u odnosu na trake.	- Ograničen kapacitet: Diskovi su ograničeni u kapacitetu pohranjivanja podataka u odnosu na trake.

- Pristupačnost: Podacima se može pristupiti bez posebnog uređaja, što olakšava vraćanje podataka u slučaju kvara. - Fleksibilnost: Diskovi se mogu koristiti za pohranu podataka na različitim platformama.	- Viša cijena: Diskovi su skuplji u odnosu na trake. - Osjetljivost: Diskovi su osjetljivi na fizička oštećenja i mogu se pokvariti.
Sigurnosna kopija baze podataka: Cloud backup	
Prednosti	Nedostaci
- Pristupačnost: Podaci su dostupni svugdje i u bilo koje vrijeme, što olakšava pristup i vraćanje podataka. - Skalabilnost: *Cloud backup* je skalabilan, što znači da se kapacitet pohranjivanja može povećavati ili smanjivati prema potrebi. - Automatizacija: Proces kreiranja sigurnosnih kopija može biti automatizovan, što smanjuje mogućnost zaboravljanja na kreiranja kopije. - Sigurnost: *Cloud backupi* nude viši nivo sigurnosti od različitih vrsta incidenata kao što su krađa ili požar jer podaci nisu unutar organizacije. - Naplata: *Cloud backupi* se ne naplaćuju kao licenca nego prema količini ili protoku podataka. To može bolje optimizovati troškove u odnosu na klasično lokalno skladištenje podataka.	- Internet konekcija: Potrebna je stabilna i brza internet-konekcija za kreiranje i vraćanje podataka iz *cloud backupa*. - Latencija: Proces kreiranja i vraćanja podataka iz *cloud backupa* može biti nešto sporiji u odnosu na lokalno skladištenje. - Mogućnost gubitka podataka: Iako su *cloud backupi* često zaštićeni od različitih incidenata, postoji mogućnost gubitka podataka u slučaju kvara ili neke druge nepredviđene okolnosti. - Cijena: *Cloud backupi* se obično naplaćuju prema korištenju, što može biti skuplje u slučaju velikih količina podataka. - Privatnost: S obzirom na to da se podaci ne nalaze unutar organizacije, postoji mogućnost neovlaštenog pristupa. Shodno tome, potrebno je provjeriti je li vendor sigurnosno pouzdan i jesu li podaci adekvatno zaštićeni.
Inkrementalni backup	
Prednosti	Nedostaci
- Ušteda vremena: Proces kreiranja inkrementalnog *backupa* traje manje vremena jer se pohranjuju samo promjene od posljednjeg *backupa*. - Ušteda prostora: inkrementalni *backup* zauzima manje prostora na disku jer se	- Ovisnost o cjelokupnom *backupu*: Da bi se vratili podaci, potreban je posljednji cjelokupni *backup* i svi naknadni inkrementalni *backupi*.

pohranjuju samo promjene u odnosu na prethodni *backupa*. - Brzo vraćanje podataka: Vraćanje podataka je brže jer se koristi cijeli posljednji *backup* i svi njegovi inkrementali.	- Kompleksan: Proces vraćanja podataka može biti kompleksan jer je potrebno vratiti sve inkrementalne *backupe*.
Diferencijalni backup	
Prednosti	Nedostaci
- Jednostavnost: Proces kreiranja i vraćanja podataka je jednostavniji u odnosu na inkrementalni *backup* jer se pohranjuju promjene od posljednjeg cjelokupnog *backupa*. - Neovisnost o cjelokupnom *backupu*: kod diferencijalnog pristupa podaci se mogu vratiti čak i ako se cjelokupni *backup i*zgubi ili ošteti.	- Potrošnja prostora: diferencijalni *backupi* zauzimaju više prostora za pohranu jer se pohranjuju promjene od posljednjeg „full“ *backupa*. - Sporije vraćanje podataka: Vraćanje podataka može biti sporije u odnosu na inkrementalni *backup.*
Mirroring backup	
Prednosti	Nedostaci
- *Real-time backup*: *Mirroring* podrazumijeva da se podaci kopiraju u stvarnom vremenu, što znači da uvijek postoje sigurnosne kopije. - Visoka dostupnost: *Mirroring* osigurava visoku dostupnost podataka jer se podaci kopiraju na drugi uređaj paralelno s radom na originalu. - Brzo vraćanje podataka: Vraćanje podataka je brzo jer se podaci mogu preuzeti s drugog uređaja odmah nakon kvara ili gubitka podataka na originalnom uređaju.	- Visoki troškovi: Mirroring zahtijeva dva uređaja za pohranu podataka, što može biti skuplje u odnosu na druge tehnologije. - Ograničena fleksibilnost: *Mirroring* ograničava fleksibilnost jer podaci moraju biti pohranjeni na dva identična uređaja.

RAID tehnologija	
Prednosti	Nedostaci
- Poboljšanje performansi: RAID kroz paralelni pristup podacima te pohranu na više diskova znatno poboljšava performanse. - Skalabilnost: RAID podržava skalabilnost jer se kapacitet pohranjivanja može povećavati dodavanjem novih diskova. - Dostupnost: RAID omogućuje visoku dostupnost podataka jer se podaci mogu preuzeti s jednog diska ako drugi disk ima tehničkih problema u radu ili je na granici performansi. - Sigurnost podataka: kod RAID tehnologije podaci se mogu pohraniti na više diskova, što smanjuje rizik od gubitka podataka u slučaju kvara jednog diska.	- Visoki troškovi: RAID zahtijeva više diskova za pohranu podataka, što može biti skuplje u odnosu na druge tehnologije. - Ovisnost o kontroleru: RAID je ovisan o kontroleru, što znači da, ako kontroler nije dostupan ili ima problema u radu, svi diskovi postaju neupotrebljivi. - Kompleksnost: Proces konfiguracije i održavanja RAID sistema može jako biti kompleksan u ovisnosti od vrste RAID sistema. Iz tog razloga potrebno je visoko znanje o ovim sistemima.
Replikacija podataka	
Prednosti	Nedostaci
- Povećana dostupnost: Replikacijom podataka se osigurava da podaci budu dostupni na više lokacija, što smanjuje rizik gubitka podataka u slučaju kvara na jednom od mjesta. - Povećana sigurnost: Replikacijom podataka se osigurava da se podaci ne gube u slučaju katastrofe ili drugog neplaniranog događaja. - Povećana performansa: Replikacijom podataka korisnici mogu pristupati podacima s više lokacija, što također može poboljšati performanse same aplikacije.	- Latencija: Replikacija podataka može uzrokovati latenciju, što znači da će korisnici morati čekati duže da pristupe podacima. - Visoki troškovi: Replikacija podataka može biti skupa, posebno ako se koriste napredni alati za replikaciju. - Komplikacije u upravljanju: Upravljanje repliciranim podacima može biti komplikovano, posebno ako se koristi više mjesta za replikaciju. - Sigurnosne mjere - replicirani podaci trebaju biti zaštićeni od neautorizovanog pristupa i promjene

Izvori: Turban et al., (2013), Bajgoric, (2009) , Whitman, Mattord, (2021), Petković, (2020), Held, (2000), Elmasri, Navathe, (2015), Koren, Krishna, (2007), Chauhan, (2014), Nelson, (2011), Buffington, (2010), Limoncelli et al., (2007).

3.4. Računarske mreže

Računarske mreže su skup povezanih računara i uređaja koji komuniciraju jedni s drugima koristeći određene protokole i standarde, a ključni su element modernog svijeta, omogućujući komunikaciju i razmjenu podataka (Tanenbaum, 2003). One su važne za poslovni kontinuitet jer ostvaruju razmjenu informacija i podataka između različitih dijelova organizacije. To znači da ako se jedan dio mreže zaguši ili prekine, drugi dio može nastaviti s radom i osigurati kontinuitet poslovanja (Bauer *et al*., 2012).

Računarske mreže se mogu podijeliti u tri glavne kategorije: lokalne mreže (LAN), širokopojasne mreže (WAN) i internet. LAN-ovi su mreže koje se koriste za povezivanje računara koji su u blizini jedni drugih, kao što je mreža u kancelariji ili školi. One postoje kako bi korisnici dijelili datoteke, uređaje i druge resurse. WAN-ovi su mreže koje se koriste za povezivanje računara na različitim lokacijama, kao što je povezivanje kancelarija u različitim gradovima ili državama. Internet je najveća mreža na svijetu, povezuje milijarde računara i uređaja širom svijeta (Limoncelli *et al*., 2007).

Postoje različite tehnologije koje omogućavaju kontinuitet poslovanja u računarskim mrežama, uključujući:

- Redundantnost – predstavlja korištenje višestrukih mrežnih uređaja koji se automatski uključuju u slučaju kvarova na primarnim uređajima. Neke od mogućih implementacija redundancije (Oggerino, 2001):
    - Redundantni ruteri i ostali mrežni elementi: preusmjeravanje i kontrola mrežnog saobraćaja će nastaviti ako se desi kvar.
    - Redundantni serveri: procesiranje podataka i komunikacija će se nastaviti u slučaju preopterećenosti mreže.
    - Redundantni pristupni linkovi: osiguravaju da se podaci prenose preko više fizičkih linkova, što smanjuje rizik od gubitka podataka u slučaju kvara jednog linka.
    - Redundantna napajanja - osigurava se kontinuitet poslovanja u slučaju kvara na izvoru napajanja.
    - Redundantni data centar - korištenjem višestrukih data centara podaci i aplikacije se spremaju na udaljenim serverima kojima se može pristupiti s bilo kojeg mjesta, što osigurava kontinuitet poslovanja u slučaju katastrofe.
    - Redundantni SAN (*Storage Area Network*) - korištenjem višestrukih SAN-ova, podaci se spremaju na više mjesta i tako se osigurava kontinuitet poslovanja u slučaju kvara.
- Dvostruka lokacija - korištenjem dvije ili više lokacija za podatke i aplikacije osigurava da se podacima može pristupiti čak i u slučaju katastrofe na jednoj lokaciji (Oggerino, 2001).
- VPN - korištenjem *Virtual Private Networka* se sigurno povezuju udaljena radna mjesta te mobilni uređaji radnika s poslovnom mrežom (Kurose, Ross, 2021).

- *Firewall* uređaji i softveri – koriste se za filtriranje i blokiranje neželjenog prometa u računarskoj mreži. Postoji više vrsta *firewalla* (Peterson, Davie, 2022):
    - *Firewall* kao fizički uređaji: često se koriste kao prva linija odbrane protiv hakerskih napada i drugih sigurnosnih prijetnji. Neki primjeri *firewall* uređaja su *Cisco ASA, Juniper SRX, Fortinet FortiGate, Dell SonicWall* itd.
    - *Firewall* kao softverski programi: Instaliraju se na računar ili server i koriste se za filtriranje i blokiranje neželjenog prometa. Oni se često koriste kao dodatna zaštita ili kao alternativa fizičkim *firewall* uređajima. Neki primjeri firewall softvera su: *Windows Firewall, iptables (Linux), pfSense, ZoneAlarm, Comodo Firewall*.
    - *Web Application Firewall* (WAF): Sigurnosni sistem koji štiti web-aplikacije od različitih vrsta web napada, kao što su *SQL injection* i *Cross-site scripting* (XSS) napadi. On se instalira između web-aplikacije i mreže. Također, filtrira i blokira neželjeni web-promet prema specifičnim pravilima i sigurnosnim politikama. Neki od WAF sistema su: *Azure Web Application Firewall, AWS WAF, Cloudflare WAF, Nginx i HAProxy.*
- Sigurnosni alati - u kontekstu računarskih mreža su softverski programi ili uređaji koji se koriste za zaštitu mreže od različitih sigurnosnih prijetnji. Oni se koriste zajedno s *firewallom* za pružanje višestruke zaštite mreži. Neki od sigurnosnih alata koji se koriste u računarskim mrežama su (Kurose, Ross, 2021):
    - Antivirusni programi (*Norton, Kaspersky, McAfee*): koriste se za skeniranje i uklanjanje virusa, crva i drugih zlonamjernih programa iz računara.
    - Anti-malware programi (*Malwarebytes, HitmanPro, AdwCleaner*): koriste se za skeniranje i uklanjanje *malwarea* (maliciozni software) koji može izazvati štetu na računaru ili mreži.
    - *Intrusion Detection and Prevention System - IDPS (Snort, Suricata)*: koristi se za detekciju i prevenciju neželjenih napada na mrežu.
    - *Vulnerability Scanner (Nessus, OpenVAS, Qualys)*: koristi se za skeniranje mreže i računara radi detekcije slabih tačaka i ranjivosti, što može iskoristiti napadač.
    - Softveri za enkripciju (*BitLocker, VeraCrypt*): koriste se za šifriranje podataka koji se prenose putem mreže, što povećava sigurnost podataka.
    - *Password management* (*LastPass, Dashlane, 1Password*): koristi se za upravljanje lozinkama, kao što su generisanje sigurnih lozinki, spremanje lozinki i automatski unos lozinki.
- Sistemi za upravljanje mrežom (*Network Management Systems* ili NMS) – jesu softverski programi ili uređaji koji se koriste za upravljanje, nadzor i dijagnostiku računarskih mreža. Kroz njih administratori prate stanje na mreži, otkrivaju i rješavaju probleme i optimizuju performanse. Primjeri NMS-a su: *SolarWinds, Nagios, PRTG Network Monitor, ManageEngine OpManager, IBM Tivoli Network Manager, HPE Network Node Manager* (Peterson, Davie, 2022).

- *Load balancer* (LB) – jeste softverski ili hardverski uređaj koji se koristi za raspodjelu opterećenja između više računara u računarskoj mreži. On je zaslužan za prenos podataka koji se šalju na mrežu, te njihovu raspodjelu između više servera, čime se osigurava da se svaki server koristi optimalno te da se spriječi preopterećenje. Time se povećava i dostupnost i skalabilnost mreže, što smanjuje rizik od preopterećenja jednog uređaja ili servera te se time dodatno osigurava kontinuitet poslovanja. Postoji više vrsta LB alata, kao što su (Lee, 2005):
    - *DNS Load Balancer*: koristi DNS za raspodjelu prometa između više servera.
    - *Hardware Load Balancer*: fizički uređaj koji se koristi za raspodjelu prometa između više servera.
    - *Software Load Balancer*: softverski program koji se koristi za raspodjelu prometa između više servera.
    - *Cloud Load Balancer*: koristi se u *cloud* okruženjima za raspodjelu prometa između više servera.
    - *Application Load Balancer*: specijaliziran za raspodjelu prometa na aplikacijskom nivou.
    - Primjeri LB alata su: *HAProxy, NGINX, F5 BIG-IP, AWS Elastic Load Balancer (ELB), Azure Load Balancer, Google Cloud Load Balancer*.
- Virtualizacija i *Cloud* - Računarske mreže su temelj za implementaciju ovih tehnologija. Više o ovome će biti rečeno u narednim poglavljima rada.

Prednosti i nedostaci implementacije navedenih tehnologija računarskih mreža se nalaze u tabeli 4:

Tabela 4. Komparacija tehnologija računarskih mreža

Redundancija računarskih mreža	
Prednosti	Nedostaci
- Sigurnost: korištenjem višestrukih mrežnih uređaja i rutera, smanjuje se rizik od prekida usluge ili gubitka podataka u slučaju kvarova. - Dostupnost: osigurava kontinuitet poslovanja kroz automatizovano preusmjeravanje prometa na drugi uređaj u slučaju kvarova. - Fleksibilnost: lakše skaliranje mreže u slučaju povećanja opterećenja.	- Troškovi: povećavaju se troškovi za njihovu kupovinu, instalaciju i održavanje. - Složenost: povećava se složenost mreže, što zahtijeva više vremena i znanja za njeno upravljanje. - Potrošnja energije: povećava se potrošnja energije, što dovodi do povećanih troškova za energiju.

Dvostruka lokacija	
Prednosti	Nedostaci
- Sigurnost: korištenjem dvije ili više lokacija za podatke i aplikacije, smanjuje se rizik od gubitka podataka u slučaju katastrofe na jednoj lokaciji. - Fleksibilnost: korištenjem dvije ili više lokacija za podatke i aplikacije, omogućava se lakše skaliranje mreže u slučaju povećanja opterećenja. - Dostupnost: korištenjem dvije ili više lokacija za podatke i aplikacije, ostavlja se mogućnost za pristup podacima i aplikacijama s bilo koje lokacije, što osigurava kontinuitet poslovanja.	- Latencija: u slučaju da se dvije lokacije nalaze u različitim regijama ili državama, moguće je da će se javiti problemi s latencijom prilikom pristupanja podacima i aplikacijama sa druge lokacije. - Troškovi: korištenjem dvije ili više lokacija za podatke i aplikacije, povećavaju se troškovi za njihovu izgradnju i održavanje. - Povećana složenost: korištenjem dvije ili više lokacija za podatke i aplikacije, povećava se složenost mreže, što zahtijeva više vremena i znanja za njeno upravljanje.
VPN	
Prednosti	Nedostaci
- Privatnost: VPN omogućuje korisnicima da se anonimno povežu na mrežu, što smanjuje rizik od praćenja ili cenzure. - Sigurnost: VPN koristi enkripciju za zaštitu podataka koji se prenose putem mreže, što smanjuje rizik od krađe podataka ili hakerskog napada. - Pristup udaljenim resursima: korisnici mogu pristupiti resursima mreže iz bilo kojeg mjesta s internetom, što osigurava rad od kuće ili rad u toku putovanja. - Smanjenje troškova: korištenjem VPN-a kompanije mogu izbjeći troškove vezane za posebne konekcije ili opremu za povezivanje filijala.	- Usporavanje brzine: Enkripcija podataka i preusmjeravanje prometa kroz VPN usporavaju brzinu mreže. - Kompleksnost konfiguracije: Podešavanje i održavanje VPN-a može biti zahtjevno u zavisnosti od potreba i veličine organizacije. - Troškovi: Korištenje VPN-a može biti skupo, posebno ako se koristi kao usluga vendora. - Ograničenja: Neki VPN-ovi mogu imati ograničenje kapaciteta ili brzine, što može utjecati na performanse mreže.
Firewall uređaji, softveri i sigurnosni alati	
Prednosti	Nedostaci
- Detekcija i prevencija: *Firewall* i sigurnosni alati mogu automatski detektirati	- Cijena: Postavljanje i održavanje *firewalla* i sigurnosnih alata može biti skupo.

i blokirati sumnjive aktivnosti, što pomaže u prevenciji napada i štiti mrežu od rizika. - Kontrola pristupa: administratori mreže mogu kontrolisati pristup resursima mreže i ograničiti pristup prema određenim kriterijima, kao što su IP adresa ili vrijeme trajanja pristupa. - Povećana sigurnost: koriste se za filtriranje i blokiranje neželjenog prometa, što smanjuje rizik od hakerskih napada i krađe podataka.	- Kompleksnost konfiguracije: Podešavanje *firewalla* i sigurnosnih alata može biti kompleksno i zahtijevati stručno znanje. - Usporavanje brzine: *Firewall* i sigurnosni alati mogu usporiti mrežu zbog filtriranja i pregledavanja prometa. - Nedostatak fleksibilnosti: *Firewall* i sigurnosni alati mogu imati ograničenja u pogledu fleksibilnosti i mogućnosti prilagodbe prema potrebama korisnika.
Sistemi za upravljanje mrežom	
Prednosti	Nedostaci
- Centralizovano upravljanje: NMS omogućava administrativnom osoblju da upravlja različitim uređajima na mreži s jednog mjesta, što smanjuje potrebu za fizičkim pristupom svakom uređaju posebno. - Automatizacija: NMS nudi mogućnost automatizacije rutinskih zadataka, kao što su konfiguracija, ažuriranje i monitoring uređaja na mreži. - Prikaz stanja mreže: kroz NMS administrativno osoblje može pratiti stanje mreže u stvarnom vremenu te pravovremeno reagovati na sve probleme. - Sigurnost: NMS omogućava administrativnom osoblju da kontroliše pristup mreži i da se zaštiti od neautorizovanih pristupa.	- Visoka ovisnost o mreži: NMS je uglavnom ovisan o radu mreže, što znači da ako mreža ne radi ispravno, NMS se ne može koristiti za upravljanje mrežom. - Trošak: Kupovina i održavanje NMS-a može biti skupo, posebno za manje mreže. - Složenost: NMS može biti složen za konfigurisanje i korištenje, što zahtijeva određeno vrijeme i iskustvo. - Ovisnost o softveru: Mreža ovisi o radu NMS-a, što znači da ako NMS ne radi ispravno, mreža može biti oštećena.
Load balanceri	
Prednosti	Nedostaci
- Raspodjela opterećenja: *Load balancer* raspoređuje zahtjeve korisnika između više	- *Single point of failure*: ako se *load balancer pokvari*, nijedan korisnik neće moći pristupiti usluzi.

servera kako bi se smanjilo opterećenje pojedinačnog servera. - Dostupnost: *Load balancer* vrši preusmjeravanje zahtjeva na druge servere ako se jedan server pokvari ili prestane raditi, što povećava dostupnost usluge. - Skalabilnost: *Load balancer* omogućava jednostavno dodavanje novih servera kako bi se prilagodio rastućem opterećenju. - Poboljšanje sigurnosti: *Load balancer* može se koristiti za filtriranje i blokiranje neželjenih zahtjeva, što povećava sigurnost mreže.	- Visoki troškovi: *Load balanceri* su skupi uređaji koji zahtijevaju posebnu konfiguraciju i održavanje. - Ograničenja: *Load balanceri* imaju ograničenja u pogledu brzine i kapaciteta, što može biti problem kod većeg opterećenja. - Složenost: *Load balanceri* su složeni uređaji koji zahtijevaju stručno znanje za konfiguraciju i održavanje.

Izvori: Hunter et al., (2019); Jader et al., (2019); Kurose, Ross, (2021); Lee, (2005); Oggerino, (2001); Peterson, Davie, (2022); Oggerino, (2001)

3.5. Cyber-sigurnost

Sigurnost u modernom računarskom okruženju postaje sve važnija tema u svijetu tehnologije i informacija. Sve više podataka i informacija se pohranjuje i prenosi putem računara i interneta, što te podatke i informacije čini izuzetno vrijednim, ali istovremeno i izuzetno ranjivim (Snedaker, 2007). *Cyber*-sigurnost kao pojam ne spada u tehnologije za kontinuirani kompjuting, ali povećanjem *cyber*-sigurnosti štiti se organizacija od hakerskih napada i drugih vrsta kibernetičkog kriminala te se tako smanjuje mogućnost prekida poslovanja. Hakeri koriste različite metode, poput *phishinga*, *malwarea* i *ransomwarea*, kako bi pristupili osjetljivim podacima i informacijama. Ova vrsta napada može imati ozbiljne posljedice na sigurnost kompanije, čak i proizvesti finansijske štete, prekinuti poslovanje, može uzrokovati gubitak podataka o klijentima, finansijama ili poslovnim procesima (Turban *et al*., 2013).

Cilj *cyber*-sigurnosti jeste da postigne sljedeće (Turban *et al*., 2013):

- učini podatke i dokumente dostupnima 24/7, ali istovremeno da ima kontrolu i ograničavanje pristupa,
- implementira i provodi procedure i politike upotrebe podatka, mreže, hardvera i softvera koji su u vlasništvu kompanije ili zaposlenih,
- promoviše sigurnu i zakonitu razmjenu informacija među ovlaštenim licima i partnerima,
- osigura usklađenost s državnim propisima i zakonima,
- spriječi napade implementiranjem nekih od tehnologija za zaštitu mreže i podataka,

- otkrije, dijagnosticira i reaguje na incidente i napade u stvarnom vremenu,
- održava interne kontrole kako bi se spriječilo neovlašteno mijenjanje podataka i zapisa,
- brz oporavak od poslovnih katastrofa i prekida.

Računarske mreže i *cyber*-sigurnost su direktno povezani jer se mreže koriste za prenos podataka i informacija, a *cyber*-sigurnost se koristi za zaštitu tih podataka i informacija od kibernetičkih napada i drugih vrsta kibernetičkog kriminala. U prethodnom poglavlju o računarskim mrežama su navedene neke od tehnologija koje se primjenjuju za održavanje kontinuiteta poslovanja u segmentu računarskih mreža. Te tehnologije zapravo spadaju u *cyber*-sigurnost – *firewall*, antivirusni programi, IDPS, enkripcija itd. Međutim, pored navedenih, postoji još tehnologija *cyber*-sigurnosti i metoda koje omogućavaju kontinuitet poslovanja:

- SIEM (*Security Information and Event Management*) jeste tehnologija kroz koju se vrši centralizovano praćenje i analiza sigurnosnih događaja u organizaciji. SIEM koristi alate za automatizovano prikupljanje podataka iz različitih sigurnosnih izvora, poput *firewalla*, antivirusnih programa, IDS/IPS-a, i drugih sigurnosnih sistema. Prikupljeni podaci se onda analiziraju kako bi se identifikovali potencijalni sigurnosni incidenti ili anomalije. SIEM sistem, također, omogućava kreiranje alarma za specifične sigurnosne događaje, kao i generisanje izvještaja o sigurnosnim incidentima i analize sigurnosnih trendova. Neki od SIEM softvera su: *IBM QRadar SIEM, Microsoft Azure Sentinel, McAfee Enterprise Security Manager* (Whitman, Mattord, 2021).
- DLP (*Data Loss Prevention*) jeste tehnologija koja se koristi za zaštitu podataka od neovlaštenog preuzimanja, kopiranja ili mijenjanja istih. To se postiže identifikovanjem, praćenjem i blokiranjem osjetljivih podataka i informacija koji se prenose, pohranjuju ili kopiraju u organizaciji, što pomaže u održavanju kontinuiteta poslovanja i zaštiti osjetljivih podataka i informacija. Primjeri DLP softvera: *Endpoint Protector, NinjaOne Backup, ManageEngine DLP Plus, McAfee DLP, Symantec DLP* (Moschovitis, 2018).
- Dvostruka autentifikacija (*Two-factor authentication*): ovom tehnologijom se osigurava da samo ovlaštene osobe mogu pristupiti osjetljivim podacima i informacijama, što pomaže u zaštiti od neovlaštenog pristupa. Dvostruka autentifikacija je metoda autentifikacije koja zahtijeva od korisnika da prođe kroz dva koraka za provjeru identiteta. Ova metoda kombinuje dva različita mehanizma za provjeru identiteta, kao što su korisničko ime i lozinka te druge metode kao što su token, SMS kod, ili biometričke metode (Stamp, 2011).
- PAM (*Privileged Access Management*) jeste tehnologija koja se koristi za kontrolu i ograničavanje pristupa osjetljivim podacima i informacijama u organizaciji. To se postiže identifikovanjem i kontrolom privilegovanog pristupa, koji se koristi za administrativne i kritične aktivnosti u IT sistemima. Primjeri PAM softvera su: *CyberArk, BeyondTrust, Centrify, Dell One Identity Manager* (Haber, 2020).

- *Vulnerability Management* je proces identifikovanja, analiziranja i ispravljanja sigurnosnih propusta (*vulnerabilities*) u sistemima i softveru. To se postiže korištenjem alata za skeniranje i analizu sigurnosnih propusta (*Vulnerability Scanners*) te praćenjem i ažuriranjem sigurnosnih propusta u različitim računarskim sistemima i softverima. Primjeri ovih softvera su: *Nessus, Qualys, OpenVAS, Nmap, McAfee Vulnerability Manager* (Brooks *et al*., 2018).

Prednosti i nedostaci implementacije navedenih tehnologija *cyber*-sigurnosti se nalaze u tabeli 5:

Tabela 5. Komparacija tehnologija za cyber-sigurnost

SIEM (Security Information and Event Management)	
Prednosti	Nedostaci
- Praćenje sigurnosnih događaja: SIEM sistem omogućuje centralizovano praćenje sigurnosnih događaja iz različitih izvora, što pomaže u bržem otkrivanju i reakciji na sigurnosne incidente. - Automatizovana analiza podataka: SIEM sistem koristi alate za automatizovanu analizu podataka kako bi se identifikovali potencijalni sigurnosni incidenti ili anomalije. - Kreiranje alarma: SIEM sistem omogućuje kreiranje alarma za specifične sigurnosne događaje, što pomaže u brzoj reakciji na sigurnosne incidente. - Generisanje izvještaja: SIEM sistem može generisati izvještaj o sigurnosnim incidentima i analizi sigurnosnih trendova, što pomaže organizaciji da bolje razumije svoje sigurnosne rizike.	- Prevelik broj lažnih alarma: SIEM sistem može generisati prevelik broj lažnih alarma, što može smanjiti učinkovitost i povećati troškove održavanja. - Ovisnost o kvaliteti podataka: SIEM sistem je ovisan o kvaliteti podataka koji se koriste za analizu, što može umanjiti njegovu učinkovitost ako podaci nisu precizni ili kompletni. - Visoki troškovi: SIEM sistem može biti skup za implementaciju i održavanje, što može biti problem za neke organizacije. - Zaostajanje za novim tehnologijama: SIEM sistem može zaostajati za novim tehnologijama i sigurnosnim trendovima, što može umanjiti njegovu učinkovitost. - Složenost konfiguracije i održavanja: SIEM sistem može biti složen za konfigurisanje i održavanje, što zahtijeva stručno znanje i iskustvo.

DLP (Data Loss Prevention)	
Prednosti	Nedostaci
- „Compliance“: pomaže organizacijama da se pridržavaju regulatornih zahtjeva i standarda za zaštitu podataka. - Identifikacija rizika: DLP omogućuje organizacijama da prepoznaju i otkriju potencijalne rizike koji bi mogli dovesti do gubitka podataka. - Zaštita podataka: osigurava organizacijama da zaštite svoje kritične podatke od neovlaštenog pristupa ili kopiranja.	- Ograničenja u performansu: DLP sistemi mogu utjecati na performanse mreže i aplikacije. - Visoki troškovi: Implementacija i održavanje DLP-a mogu biti skupi. - Složenost: DLP sistemi mogu biti složeni za upravljanje i konfigurisanje. - False-positive: DLP sistemi mogu generisati lažne alarmne signale, što može dovesti do prekomjerne intervencije i gubitka produktivnosti.
Dvostruka autentifikacija	
Prednosti	Nedostaci
- Smanjenje rizika od *phishinga*: Dvostruka autentifikacija smanjuje rizik od *phishinga* jer korisnik mora potvrditi svoj identitet koristeći dva različita kanala, što značajno smanjuje mogućnost da lažni ili neovlašteni korisnik pristupi računu. - Sigurnosti standard: Dvostruka autentifikacija pomaže organizacijama da se pridržavaju regulatornih zahtjeva i standarda za sigurnost podataka. - Povećana sigurnost: Dvostruka autentifikacija povećava sigurnost jer zahtijeva da korisnik potvrdi svoj identitet koristeći dva različita kanala (npr. šifru i jednokratni kod) prije nego što može pristupiti određenom računu ili usluzi.	- Poteškoće pri korištenju: Dvostruka autentifikacija može biti teška za korištenje, posebno za korisnike koji nisu navikli na ovaj pristup. - Dodatni troškovi: Dvostruka autentifikacija može povećati troškove za organizaciju jer se treba kupiti i implementirati dodatni softver ili hardver. - Mogućnost zloupotrebe: Dvostruka autentifikacija može biti zloupotrijebljena ako se koristi jednokratni kod koji se može lahko preuzeti ili kupiti.

PAM (Privileged Access Management)	
Prednosti	Nedostaci
- Poboljšana produktivnost: PAM omogućuje organizacijama da automatizuju procese kontrole pristupa privilegovanim korisničkim računima i resursima, što može poboljšati produktivnost. - Poboljšana kontrola: kroz PAM organizacije mogu kontrolisati i pratiti korištenje privilegovanih korisničkih računa i resursa. - Regulatorni zahtjevi: PAM pomaže organizacijama da se pridržavaju regulatornih zahtjeva vezanih za kontrolu pristupa privilegovanim korisničkim računima i resursima.	- Poteškoće u praćenju korištenja privilegovanih korisničkih računa: PAM sistemi se moraju temeljiti na podacima o korištenju privilegovanih korisničkih računa, što može biti teško za praćenje i analiziranje, posebno u velikim organizacijama. - Poteškoće u održavanju: PAM sistemi zahtijevaju redovno održavanje kako bi se osigurala njihova funkcionalnost i sigurnost. - Poteškoće u integraciji s postojećim sistemima: PAM sistemi se mogu teško integrisati s postojećim IT sistemima organizacije.
Vulnerability Management	
Prednosti	Nedostaci
- Automatizacija: omogućuje automatizovano skeniranje, praćenje i upravljanje ranjivostima u okruženju. - Brza detekcija: kroz *Vulnerability Management* je moguće brzo otkriti ranjivosti, što za rezultat ima jednako brzu reakciju i smanjenje rizika. - Povećana sigurnost: povećava sigurnosti okruženja tako što identifikuje i ispravlja ranjivosti prije nego što budu iskorištene od napadača. - Efikasnost: kroz centralizovano upravljanje i praćenje povećava efikasnost upravljanja ranjivostima u cijelom okruženju.	- Troškovi: alati mogu biti skupi, što može predstavljati problem za manje organizacije ili organizacije s ograničenim budžetom. - *False positive*: Alati mogu generisati lažne pozitivne rezultate, što zahtijeva dodatnu provjeru i analizu. - Manjak funkcionalnosti: ne pokriva sve vrste ranjivosti ili ne podržava sva okruženja, što može predstavljati problem za organizacije koje koriste različite vrste tehnologije.

Izvori: Sheeraz et al., (2023); Stamp (2011); Moschovitis (2018); Haber (2020); Brooks et al. (2018); Whitman, Mattord, (2021); Turban et al. (2013); Snedaker (2007).

3.6. Cloud computing i virtualizacija

Cloud computing je revolucionarni koncept koji kompanijama i pojedincima omogućava da pristupe računarskim resursima i uslugama putem interneta, iz bilo kojeg mjesta i u bilo kojem trenutku. Dakle, to je tehnologija putem koje preduzeća mogu koristiti IT resurse (poput aplikacija, skladištenja podataka, računara i usluga) putem interneta, umjesto da ih imaju na svom lokalnom računaru ili u vlastitom poslovnom okruženju (Rittinghouse, Ransome, 2010).

Jedna od glavnih prednosti korištenja *clouda* je fleksibilnost. Kompanije mogu prilagoditi količinu resursa koje koriste prema svojim potrebama, tako da ne moraju plaćati za neiskorištene resurse kao što su memorija, procesori, mreža, električna energija itd. Osim toga, kompanije ne moraju brinuti o održavanju i nadzoru IT infrastrukture te se mogu fokusirati na svoje ključne poslovne aktivnosti. *Cloud computing* također omogućava lakšu skalabilnost. Kompanije mogu lahko proširiti ili smanjiti količinu resursa koje koriste, što za rezultat ima bolju prilagodljivost promjenama u poslu. Osim toga, *cloud computing* olakšava kompanijama da se brzo prilagode novim tehnologijama kako bi pratile tržišne trendove i ostale konkurentne (Turban, Volonino, 2011).

Međutim, *cloud computing* također ima neke nedostatke. Jedan od glavnih problema je sigurnost podataka. Kompanije moraju biti svjesne rizika od sigurnosnih propusta i imati adekvatno razvijene planove zaštite podataka od neovlaštenog pristupa, krađe i ostalih malicioznih namjera. Osim toga, trebaju biti svjesne da, neovisno o tome koliko je *cloud computing* siguran, njihovi podaci uvijek mogu biti ugroženi. (Wallace, Webber, 2018).

Postoje tri glavna tipa *cloud computing* usluga (Tanenbaum, Bos, 2014):

- IaaS (*Infrastructure as a Service*),
- PaaS (*Platform as a Service*) i
- SaaS (*Software as a Service*).

Infrastructure as a Service (IaaS) oblik je *cloud computinga* koji omogućava kompanijama da se oslobode potrebe da održavaju i skaliraju vlastitu IT infrastrukturu. Umjesto toga, kompanije koriste IaaS da unajme od vendora infrastrukturu, uključujući računare, skladištenje, mrežne usluge i druge IT resurse (Rittinghouse, Ransome, 2010). IaaS osigurava poslovni kontinuitet tako što pruža fleksibilnost i skalabilnost koja je potrebna kako bi se kompanija prilagodila promjenama u poslovanju (Snedaker, 2007).

Platform as a Service (PaaS) jeste oblik *cloud computinga* putem kojeg kompanije mogu razvijati, testirati i puštati u rad aplikacije bez potrebe za kupovinom i održavanjem hardvera i softvera. PaaS pruža okruženje za razvoj aplikacija, alate za upravljanje i infrastrukturu potrebnu za pokretanje i održavanje aplikacija (Rittinghouse, Ransome, 2010). PaaS također omogućava kompanijama da se brže prilagode promjenama u poslovnom okruženju i da bolje iskoriste nove tehnologije i alate za razvoj aplikacija (Snedaker, 2007).

Software as a Service (SaaS) jeste oblik korištenja softvera, gdje korisnici putem interneta pristupaju i koriste softver koji je pokreće i izvršava udaljenim serverima. Tako kompanije mogu koristiti softver bez potrebe da ga instaliraju i održavaju na svojim lokalnim računarima (Haber, 2020). Korištenje SaaS-a osigurava poslovni kontinuitet zato što se kompanije ne moraju brinuti o održavanju i ažuriranju softvera na vlastitim serverima. Umjesto toga, to je na snazi izdavača softvera. Također, SaaS doprinosi većoj fleksibilnosti i pouzdanosti time što kompanije mogu pristupati softveru i podacima s bilo kojeg mjesta, u bilo koje vrijeme, te je tako moguće raditi i obavljati poslovne aktivnosti s bilo koje lokacije (Snedaker, 2007).

Cloud computing omogućava poslovni kontinuitet pomoću različitih tehnologija, uključujući:

- Virtualizaciju: *Cloud computing* koristi virtualizaciju kako bi stvorio „virtuelne" IT resurse (kao što su virtuelni računari i virtuelna skladišta podataka) koji se mogu koristiti putem interneta. Virtualizacijom, fizički hardver se razdvaja od operativnog sistema i aplikacija, što za cilj ima višestruko korištenje istog hardvera i bolju iskorištenost resursa. Time preduzeća koriste IT resurse bez fizičkog pristupa mašinama, tj. glavnom serveru. Postoje različiti alati za virtualizaciju koji se koriste u *cloud computingu*, a neki od njih su: *Vmware, Hyper-V, VirtualBox, KVM, Xen* (Menken, Blokdijk, 2010).
- Automatizaciju: u oblasti *cloud computinga* predstavlja korištenje tehnologije i algoritama za automatsko upravljanje i skaliranje IT resursa u *cloud* okruženju. To uključuje automatizaciju procesa kao što su provizioniranje, konfigurisanje, održavanje i monitoring IT resursa. Automatizacija omogućava lakše skaliranje IT resursa prema potrebama poslovanja, što znači da se resursi mogu dodavati ili uklanjati u stvarnom vremenu, bez prekida u radu. Bitno je naglasiti da automatizacija smanjuje rizik od ljudskih grešaka u upravljanju IT resursima, što znači da se resursi mogu koristiti efikasnije. Primjeri alata za automatizaciju*: Puppet, Chef, Ansible, Terraform Docker, Kubernetes*. (Priyam, 2018).
- Usluge po narudžbi (engl. *pay-as-you-go*): predstavljaju način na koji se koristi *cloud computing*, gdje korisnici ne plaćaju unaprijed za kapacitet koji ne koriste, već se naplaćuje samo za resurse koji su stvarno korišteni (Tang, Lee, He, 2014). Time se povećavaju fleksibilnost i ekonomičnost, jer korisnici ne moraju kupovati i održavati IT opremu, već mogu povećati ili smanjiti kapacitet *cloud* usluge prema trenutnoj potrebi. U pogledu poslovnog kontinuiteta, *pay-as-you-go* osigurava kompanijama da lakše raspolažu IT resursima i da se lakše prilagode promjenama u poslovanju. To znači da se kompanije mogu prilagoditi promjenama u potražnji i biti spremnije na krize ili neplanirana odsustva (Barbosa, Charão, 2012).
- *Serverless* računarstvo: predstavlja arhitekturu koja omogućava izvođenje koda bez direktne kontrole nad fizičkim ili virtuelnim serverima. Umjesto toga, kod se izvršava u *serverless* okruženju, koje automatski alocira resurse potrebne za izvršavanje koda, a potom ih oslobađa kada se izvršavanje koda završi. Ova

arhitektura osigurava brži razvoj i niže troškove, jer se serveri ne moraju održavati ni plaćati. *Serverless* računarstvo se najčešće koristi za pokretanje manjih, nezavisnih dijelova aplikacije (Hunter, Porter, Rajan 2019).

Sve ove tehnologije zajedno omogućavaju preduzećima da koriste *cloud computing* kao sredstvo za održavanje poslovnog kontinuiteta, bilo da se radi o dostupnosti, automatizaciji, skalabilnosti ili sigurnosti. Prednosti i nedostaci implementacije navedenih tehnologija *cloud computinga* i virtualizacije se nalaze u tabeli 6:

Tabela 6. Komparacija cloud computing tehnologija

Virtualizacija	
Prednosti	Nedostaci
- Efikasnije iskorištavanje resursa: Virtualizacija višestruko iskorištava fizičke resurse (procesora, memorije, diskova itd.) te tako više virtuelnih mašina radi na istom fizičkom hardveru. - Olakšano upravljanje i skaliranje: Virtualizacija osigurava lakše upravljanje i skaliranje IT infrastrukture, jer se virtuelne mašine mogu lahko klonirati, migrirati i automatizovati. - Poboljšana sigurnost: Virtualizacija omogućava bolju sigurnost, jer su virtuelne mašine logički izolovane jedna od druge, što znači da problem s jednom virtuelnom mašinom neće utjecati na druge. - Razvoj i testiranje: Virtualizacija olakšava razvoj i testiranje aplikacija jer se različita okruženja mogu lahko kreirati i pokretati na virtuelnim mašinama. - Fleksibilnost: koristeći virtualizaciju, IT infrastruktura se lahko prilagođava promjenama u skladu s potrebama i poslovnim aktivnostima.	- Potreba za *backup* i *disaster recovery*: Virtualizacija zahtijeva dodatnu zaštitu podataka i infrastrukture, što zahtijeva povećanje troškova. - Trošak: Virtualizacija zahtijeva dodatne resurse (procesor, memorija itd.) za rad virtuelnih mašina, što može dovesti do povećanja troškova. - Kompleksnost: Virtualizacija može povećati kompleksnost IT infrastrukture, što može otežati upravljanje i održavanje. - Sigurnost: Virtualizacija zahtijeva povećanje sigurnosti jer se virtuelne mašine moraju izolovati jedna od druge. - Kvalifikovani ljudski resursi: Virtualizacija zahtijeva ljude s odgovarajućim znanjem i vještinama kako bi se efikasno upravljali i održavali virtuelno okruženje.

Automatizacija	
Prednosti	Nedostaci
- Povećana efikasnost: kroz automatizaciju rutinskih poslova i procesa povećava se efikasnost te smanjuju poslovni troškovi. - Poboljšana skalabilnost: Automatizacija omogućava lakše skaliranje resursa u skladu s potrebama poslovanja, što dovodi do poboljšanja performansi i smanjenja troškova. - Olakšano upravljanje: Automatizacija olakšava upravljanje IT infrastrukturom, što smanjuje mogućnost ljudske greške, a time se poboljšavaju kontrola i nadzor sistema i poslovnih procesa. - Poboljšana sigurnost: Automatizacija omogućava bolju sigurnost, jer se procesi automatizuju i lakše kontrolišu, što dovodi do smanjenja rizika.	- Skupa implementacija: Implementacija automatizacije može biti skupa i zahtijevati velika ulaganja u tehnologiju i stručnjake. - Ovisnost o tehnologiji: Prevelika ovisnost o automatizaciji može dovesti do problema u slučaju kvarova ili prekida u tehnologiji. - Ograničenja u fleksibilnosti: Automatizacija može ograničiti fleksibilnost u radu i otežati prilagodbu promjenama u okruženju. - Nedostatak ljudske intervencije: Prevelika automatizacija može dovesti do smanjene ljudske intervencije, što može dovesti do problema u slučaju neočekivanih situacija.
Usluge po narudžbi (pay-per-use)	
Prednosti	Nedostaci
- Fleksibilnost: Korisnici mogu prilagoditi svoje računarske resurse shodno trenutnim potrebama. - Smanjenje troškova: Korisnici ne moraju investirati u skupe IT infrastrukture i mogu platiti samo za ono što koriste. - Skalabilnost: Usluge po narudžbi omogućavaju korisnicima da brzo reaguju na promjene u potražnji i da se prilagode promjenama u okruženju. - Dostupnost: Usluge po narudžbi su dostupne globalno i korisnici mogu pristupiti resursima iz bilo kojeg mjesta.	- Ovisnost o internetu: Korisnici su ovisni o kvaliteti internet-veze za pristup *cloud* resursima. - Nedostatak kontrole: Korisnici imaju ograničenu kontrolu nad resursima i ne mogu prilagoditi svoje potrebe prema specifičnim zahtjevima. - Nedostatak sigurnosti: Usluge po narudžbi ne daju isti nivo sigurnosti kao vlastita IT infrastruktura i korisnici su ovisni o sigurnosti pružatelja usluga.

Serverless računarstva	
Prednosti	Nedostaci
- Niži troškovi: organizacije ne moraju plaćati za održavanje servera, što znači da se troškovi smanjuju u skladu s količinom resursa koji se koristi. - Povećana fleksibilnost: *Serverless* računarstvo omogućava da se kod izvodi u različitim okruženjima, što znači da se aplikacije mogu razvijati i izvoditi na više platformi. - Skalabilnost: *Serverless* računarstvo olakšava skaliranje resursa u skladu s potrebama aplikacije i korisnika. - Automatizacija: *Serverless* okruženja automatizuju mnoge aspekte infrastrukture, uključujući raspodjelu resursa, održavanje, i sigurnost.	- Ograničenja u performansama: Izvođenje koda u okruženju s ograničenim resursima može dovesti do performansi nižih od onih koje se mogu postići direktnom kontrolom nad serverima. - Ograničenja u kapacitetu: Serverless okruženja imaju ograničenja u kapacitetu, što znači da se ne mogu koristiti za aplikacije s velikim potrebama za resursima. - Visoki troškovi: Ako se velike količine podataka prenose ili čuvaju u okruženju, troškovi mogu biti visoki. - Ograničenja u razvoju: *Serverless* okruženja imaju ograničenja u razvoju, što znači da se ne mogu koristiti za aplikacije s kompleksnim potrebama.

Izvori: Wang et al. (2015); Al-Jahdali et al., (2014); Haber, (2020); Hunter, Porter, Rajan (2019); Priyam, (2018); Menken, Blokdijk, (2010); Rittinghouse, Ransome, (2010); Barbosa, Charão, (2012); Turban, Volonino, (2011); Snedaker, (2007); Wallace, Webber, (2018); Tang, Lee, He, (2014).

3.7. Ostale nove tehnologije

Tehnologije za kontinuitet poslovanja i dalje se razvijaju i svaki dan se pojavljuju neke nove ideje i alati za brz i efikasan oporavak od katastrofalnih događaja ili nesreća. Mnogo novih tehnologija tek treba da se komercijalizuje i postane dostupno preduzećima i organizacijama. Međutim, mogu se izdvojiti sljedeće tehnologije koje su u posljednjim godinama dobile na popularnosti (Kranz, 2016; Kumari *et al*., 2022; Buyya, 2019; Hamadah, Aqel, 2019; Yang *et al*., 2021):

- „Internet stvari“ (engl. *Internet of Things* – IoT),
- „Edge“ računarstvo (engl. *edge computing*),
- „Spremnici“ (engl. *containers),*
- Oporavak od katastrofe kao usluga (engl. *Disaster Recovery as a Services* – DRaaS),
- 5G mreža

Bitno je naglasiti da navedene nove tehnologije ne možemo direktno svrstati u klasične ili primarne tehnologije za kontinuirani kompjuting. Međutim, one imaju veliki potencijal kao pomoć u osnaživanju postojećih tehnologija za kontinuirani kompjuting.

3.7.1. „Internet stvari“ (engl. *Internet of Things* – IoT)

Internet of Things (IoT) tehnologija podrazumijeva povezivanje različitih uređaja i senzora u mrežu koja se može koristiti za automatizaciju poslovnih procesa i povećanja efikasnosti. To može doprinijeti poslovnom kontinuitetu kroz bolju kontrolu nad procesima i podacima, što pomaže u prevenciji kvarova i smanjenju gubitaka. Pored toga, IoT tehnologija također može pomoći u detekciji i prevenciji potencijalnih rizika, što povećava sigurnost poslovanja (Kranz, 2016).

To se postiže korištenjem metoda i tehnologija kao što su (Hussain, 2017; Sinclair, 2017):

- Predviđanje održavanja: IoT senzori mogu se koristiti za praćenje stanja mašina, opreme i procesa u stvarnom vremenu, tj. predviđanje potencijalnih kvarova prije nego što se pojave.
- Automatizacija procesa: IoT tehnologija može se koristiti za automatizaciju poslovnih procesa poput proizvodnje, skladištenja i distribucije.
- Analitika podataka: IoT uređaji generišu veliku količinu podataka koji se mogu analizirati kako bi se dobile informacije o poslovanju i donosile bolje poslovne odluke.
- *Remote monitoring*: IoT tehnologija omogućava da se uređaji i procesi prate izdaleka, što znači da se u slučaju kvarova ili problema može intervenisati s bilo koje geografske lokacije.
- Upravljanje lancem snabdijevanja: uređaji koji podržavaju IoT kao što su RFID oznake i senzori mogu se koristiti za praćenje kretanja i stanja robe kroz lanac snabdijevanja, poboljšavajući vidljivost i efikasnost operacija.

Prednosti i nedostaci implementacije IoT tehnologije nalaze u tabeli 7:

Tabela 7. Komparacija IoT tehnologije

„Internet stvari“ (engl. *Internet of Things* – IoT)	
Prednosti	Nedostaci
- Poboljšana efikasnost: IoT uređaji mogu automatizovati procese i prikupljati podatke, omogućavajući bolje donošenje odluka i brže rješavanje problema. - Povećana produktivnost: IoT uređaji mogu daljinski nadgledati i kontrolisati	- Privatnost: IoT uređaji prikupljaju mnogo ličnih podataka koji se mogu koristiti za zloupotrebe. - Sigurnosni problemi: IoT uređaji mogu biti osjetljivi na hakiranje i *cyber* napade,

opremu, smanjujući vrijeme zastoja i povećavajući produktivnost. - Bolje prikupljanje i analiza podataka: IoT uređaji mogu prikupiti velike količine podataka, koji se mogu analizirati radi poboljšanja poslovanja i identifikovanja novih poslovnih prilika. - Ušteda: IoT uređaji mogu smanjiti potrošnju energije, što dovodi do uštede finansijskih sredstava. - Poboljšanje sigurnosti: IoT tehnologija može se koristiti za detekciju i prevenciju potencijalnih rizika, što povećava sigurnost poslovanja.	koji mogu poremetiti operacije i dovesti do gubljenja podataka. - Kompleksnost: Implementacija i održavanje IoT sistema može biti složeno i može zahtijevati specijalizovano znanje i stručnost. - Trošak: Implementacija IoT sistema može biti skupa i može zahtijevati značajna ulaganja unaprijed.

Izvori: Al-Ali et al. (2019); Kranz (2016); Hussain (2017); Sinclair (2017); Zhou, (2013); DaCosta, (2013); Hwang et al. (2011); Mukhopadhyay (2014)

3.7.2. „Edge“ računarstvo (engl. *Edge computing*)

Klasični pristup obrade podataka podrazumijeva centralizovanu lokaciju na koju se šalju svi podaci radi obrade. Međutim, *edge computing* se odnosi na koncept obrade podataka bliže ili na samom mjestu kreiranja podataka. Ovo se može postići korištenjem mrežnih uređaja kao što su ruteri ili *gatewayi,* ili korištenjem specijaliziranih *edge computing* računarskih uređaja kao što su industrijski računari ili *edge serveri*. *Edge computing* se često koristi u IoT (*Internet of Things*) sistemima, kao i u industrijskim i proizvodnim okruženjima, gdje su niske latencije i visoka pouzdanost važni (Kumari *et al*., 2022).

Edge computing može pomoći u kontinuitetu poslovanja pružanjem pouzdane i otporne arhitekture sistema. Obradom podataka na njihovom izvoru, umjesto oslanjanja na centralnu lokaciju, *edge computing* može pomoći da se poboljša pouzdanost sistema. U slučaju kvara ili prekida na centralnoj lokaciji, *edge* uređaji mogu nastaviti raditi samostalno održavajući sistem u radu, to jeste minimizira se utjecaj prekida mreže ili drugih poremećaja i osigurava da su kritični podaci i usluge i dalje dostupni korisnicima.

Edge computing, analizom podataka pri kreiranju, omogućava da se prije detektuju potencijalni problemi, što minimizira mogućnost sistemskih kvarova i čini cjelokupni sistem sigurnijim (Al-Turjman, 2019). Prednosti i nedostaci implementacije *edge computinga* nalaze se u tabeli 8:

Tabela 8. Komparacija edge computing tehnologije

„Edge“ računarstvo (engl. *edge computing*)	
Prednosti	Nedostaci
- Smanjeno kašnjenje: Obradom podataka pri njihovom kreiranju, *edge computing* može poboljšati ukupan performans i odziv aplikacije jer već obrađene podatke prosljeđuje dalje. - Poboljšana pouzdanost: Uz *edge computing*, preduzeća mogu nastaviti s radom čak i ako se veza s centralnom lokacijom izgubi, jer se podaci mogu obraditi i pohraniti lokalno na *edge* uređaju. - Povećana efikasnost: *Edge computing* može pomoći preduzećima da bolje upravljaju protokom podataka, smanjujući količinu nepotrebnih podataka koji se trebaju prenijeti preko mreže. - Uštede: *Edge computing* može pomoći preduzećima da smanje troškove povezane s održavanjem i skaliranjem centralizovane infrastrukture.	- Ograničena standardizacija: Tržište *edge computing* uređaja je još relativno novo i postoji nedostatak standardizacije među uređajima i tehnologijama. - Povećana složenost: Upravljanje distribuiranom mrežom *edge* uređaja može biti složenije od upravljanja centralizovanom infrastrukturom, zahtijevajući dodatne resurse i stručnost. - Ograničena skalabilnost: *Edge computing* rješenja možda neće moći podnijeti isti nivo volumena podataka i procesorske snage kao centralizovana rješenja, ograničavajući skalabilnost cjelokupnog sistema. - Sigurnosni rizici: *Edge* uređaji mogu biti osjetljiviji na narušavanje sigurnosti, jer se često nalaze na udaljenim ili nesigurnim lokacijama.

Izvori: Al-Turjman (2019), Kumari et al. (2022), Yang et al. (2021), Bai, Scholl, (2021), Buyya (2019), Ahmed, Haskell-Dowland (2021), Marcham (2021).

3.7.3. „Spremnici“ (engl. *Containers*)

Spremnici su virtuelna okruženja za pokretanje aplikacija. Oni se koriste za izolaciju aplikacija od okruženja u kojem se pokreću, tako da se aplikacije mogu pokrenuti bilo gdje bez problema, s kompatibilnošću. Spremnici su kreirani koristeći tehnologije *namespaces* i *control groups* koje omogućavaju da se kreira izolovano okruženje unutar operativnog sistema, u kojem se aplikacija može pokrenuti vlastitim resursima (procesori, memorija, itd.). Također, spremnici su *lightweight* (laki) i brzo se pokreću, što ih čini odličnim za *cloud* i *edge computing*. Mogu se koristiti za mnoge namjene, uključujući automatizaciju procesa instalacije i ažuriranja aplikacija, testiranje i razvoj, te puštanje aplikacija na sistem korisnika ili klijenta (Buyya, 2019). Oni mogu biti izrazito korisni za kontinuitet poslovanja, jer se aplikacije mogu lahko klonirati i replicirati u različitim okruženjima.

Spremnici također sadrže sve potrebne resurse za pokretanje aplikacije, uključujući operativni sistem, biblioteke, konfiguracije itd. To znači da se aplikacije mogu pokrenuti na bilo kojem računaru koji ima instaliran *Docker,* bez obzira na to koji operativni sistem ili verziju biblioteka koristi računar (Gkatziouras, 2022).

Docker je platforma za upravljanje spremnicima. Ona koristi tehnologiju spremnika za pokretanje aplikacija te se tako aplikacije lakše kreiraju, pokreću i kontrolišu. Docker je *open-source* i dostupan je za sve glavne operativne sisteme, uključujući *Windows*, *MacOS* i *Linux*. On omogućava kreiranje, pokretanje i upravljanje spremnicima preko komandne linije ili grafičkog korisničkog interfejsa. *Docker,* također, pruža mogućnost kreiranja i dijeljenja spremnika putem centralnog repozitorija *Docker Hub* (Menga, 2018).

Prednosti i nedostaci implementacije tehnologije „Spremnika“ nalaze se u tabeli 9:

Tabela 9. Komparacija containers tehnologije

„Spremnici“ (engl. *Containers*)	
Prednosti	Nedostaci
- Portabilnost: *Docker* spremnici mogu raditi na bilo kojoj platformi koja podržava *Docker*, što olakšava premještanje aplikacija između razvojnog, testnog i produkcionog okruženja. - Verzioniranje: *Docker* spremnici mogu biti verzionisani te se tako aplikacije lahko vraćaju na prethodnu verziju u slučaju problema. - Izolacija: Docker spremnici pružaju način za izolaciju aplikacija i njihovih ovisnosti, smanjujući rizik od sukoba između različitih aplikacija i okruženja. - Skalabilnost: Docker spremnici se mogu lahko povećati ili smanjiti kako bi zadovoljili promjenjivu potražnju.	- Kompleksnost: s obzirom na način implementacije i konfiguracije *Docker* spremnika, cjelokupan proces upravljanja aplikacijom je složeniji. - Sigurnost: Sigurnosna razmatranja treba uzeti u obzir kada se koriste *Docker* spremnici, jer oni mogu biti ranjivi na napade ako nisu pravilno konfigurisani. - Upravljanje: orkestracija i upravljanje *Docker* spremnicima može biti složeno i vremenski zahtjevno.

Izvori: Candel (2022), Gkatziouras (2022), Buyya (2019), Menga (2018), Vasavada, Sametriya (2022).

3.7.4. Oporavak od katastrofe kao usluga (engl. *Disaster Recovery as a Services*)

DRaaS je visoko efikasna usluga *cloud computinga* koja omogućava organizacijama da sigurno čuvaju podatke, aplikacije i IT infrastrukturu u pouzdanom *cloud* okruženju. To je sveobuhvatno rješenje za upravljanje cjelokupnim procesom oporavka od katastrofe putem softvera kao usluge (engl. *Software as a Services* - *SaaS*), omogućavajući preduzećima da brzo vrate pristup i funkcionalnost svojim IT sistemima nakon nepredviđene katastrofe. Usvajanjem modela „Oporavak od katastrofe kao usluga“, organizacije su oslobođene tereta posjedovanja i upravljanja svim potrebnim resursima za oporavak od katastrofe, jer se mogu osloniti na stručnost i infrastrukturu koju pruža treća strana (Hamadah, Aqel, 2019).

Kroz implementaciju DRaaS usluge, uklanja se direktni nadzor nad procesima i održavanje vlastite lokalne infrastrukture za oporavak od katastrofe te, shodno tome, kompanije mogu uštedjeti finansijska sredstva. Međutim, kompanija bi trebala dobro obratiti pažnju na stavke ugovora koje potpiše s vendorom DRaaS usluge. Potrebno je ustanoviti postoji li mogućnost da se u isto vrijeme desi nepredviđena katastrofa i kod kompanije i kod vendora usluge, te kako će to utjecati na vrijeme odaziva sistema (Prakash *et al*., 2012).

Oporavak od katastrofe, u kontekstu usluge, obično podrazumijeva (Andrade *et al*., 2017; Wood *et al*., 2010; Rehab, Sta, 2016):

- Replikaciju podataka: Organizacija definiše opseg podatka i aplikacija koje želi replicirati i šalje ih putem interneta ili nekog drugog oblika IKT mreže prema *cloud* infrastrukturi pružatelja usluga DRaaS-a. Replicirani podaci se redovno ažuriraju kako bi bili što bolje usklađeni s izvornim podacima sistema organizacije.
- Prioritete oporavka: Organizacija definiše prihvatljivo vrijeme za obnavljanje aplikacije i vraćanje pristupa podacima nakon neplaniranog prekida (engl. *Recovery Time Objective* – RTO). Definiše se količina podataka koja se potencijalno može izgubiti nakon oporavka od katastrofe, prije nego što gubitak podataka premaši ono što je prihvatljivo za organizaciju (engl. *Recovery Point Objective* - RPO).
- Testiranje i provjeru: Vendor DRaaS usluge je dužan redovno vršiti testiranja i provjere sistema oporavka kako bi se osigurala funkcionalnost i tačnost procesa.
- Aktivaciju i oporavak: U slučaju da se desi nepredviđena katastrofa te dođe do prekida poslovnih operacija, organizacija aktivira oporavak putem usluge DRaaS. Replicirani podaci se brzo preuzimaju i aplikacije se pokreću na *cloud* infrastrukturi, što predstavlja oporavak poslovnih procesa.

Prednosti i nedostaci implementacije tehnologije DRaaS nalaze se u tabeli 10:

Tabela 10. Komparacija DRaaS tehnologije

DRaaS	
Prednosti	Nedostaci
- Visoka dostupnost: DRaaS osigurava kontinuiranu dostupnost podataka i aplikacija, čak i u slučaju katastrofalnih događaja ili kvarova na glavnom sistemu. - Skalabilnost: DRaaS omogućava fleksibilnost i skalabilnost resursa prema potrebama poslovanja, pružajući mogućnost prilagodbe kapaciteta u stvarnom vremenu. - Smanjenje troškova: Korištenje DRaaS tehnologije može značajno smanjiti troškove vezane uz izgradnju i održavanje vlastitog infrastrukturnog sistema za oporavak od katastrofe. - Brz oporavak: DRaaS osigurava brz oporavak poslovnih operacija jer podaci i aplikacije brzo mogu biti vraćeni i ponovno aktivirani nakon prekida ili kvara. - Automatizacija i jednostavnost upravljanja: DRaaS pruža automatizovane procese oporavka i jednostavnost upravljanja, što olakšava implementaciju i održavanje planova oporavka od katastrofe.	- Sigurnost podataka: Uprkos visokoj sigurnosti koju pruža DRaaS, organizacije mogu biti zabrinute zbog prenošenja osjetljivih podataka preko javnih mreža ili povjerenja u sigurnost vendora usluge. - Ovisnost o vendoru usluge: Korištenje DRaaS znači da organizacija postaje ovisna o pouzdanosti i dostupnosti vendora usluge oporavka od katastrofe. - Potreba za prilagodbom: Uvođenje DRaaS tehnologije može zahtijevati promjene u postojećim procesima i pristupima, što može predstavljati izazov i zahtijevati obuku zaposlenika. - Potencijalni gubitak kontrole: Povjeravanje oporavka od katastrofe vendora usluga znači da organizacija može izgubiti određeni nivo kontrole nad postupcima i vremenom oporavka. - Kompatibilnost s postojećom infrastrukturom: Prije implementacije DRaaS-a, organizacija mora provjeriti je li njihova postojeća infrastruktura kompatibilna s tehnologijom i može li se integrisati bez većih problema.

Izvori: Prakash et al. (2012); Wood et al. (2010); Indira (2016); Saquib et al. (2013); Andrade et al., (2017); Anis Aziz, Babulak, Al-Dabass (2021); Rehab, Sta, (2016); Hamadah, Aqel (2019)

3.7.5. 5G mreža

Peta generacija (5G) mobilnih mreža je nova generacija mreže za prenos podataka. Ona pruža manje kašnjenje, tj. latenciju, veću brzinu, veću propusnost, i to do 10 puta u odnosu na prethodnu generaciju (Marcham, 2021). To omogućava brži prenos velikih količina podataka kao što su videoprenos i preuzimanje velikih datoteka. Osim toga, 5G može

podržati implementaciju IoT uređaja i korištenje *edge computing* tehnologije, što može pomoći preduzećima da optimiziraju operacije i poboljšaju efikasnost.

Dodatna karakteristika 5G mreže jeste veći broj paralelnih konekcija u odnosu na prethodnu generaciju 4G, što omogućava da više uređaja bude povezano na istu mrežu u isto vrijeme. Dakle, koristeći 5G mrežu povećava se redundantnost uređaja i propusnost na mreži (Yang *et al.*, 2021).

Tehnologija 5G može pomoći kompanijama da održe kontinuitet poslovanja, pružajući veće internetske brzine i pouzdanije veze, što osigurava rad na daljinu, obradu podataka u stvarnom vremenu i brži prijenos podataka. Prednosti i nedostaci implementacije tehnologije 5G nalaze se u tabeli 11:

Tabela 11. Komparacija 5G tehnologije

5G mreža	
Prednosti	Nedostaci
- Velike brzine: 5G mreže nude mnogo veće brzine od 4G mreža, što može pomoći u poboljšanju performansi poslovnih kritičnih aplikacija i usluga. - Niska latencija: 5G mreže imaju znatno manje kašnjenje od 4G mreža, što može pomoći u poboljšanju odziva aplikacija i usluga u stvarnom vremenu. - Povećan kapacitet: 5G mreže imaju mnogo veći kapacitet od 4G mreža, što može pomoći da se podrži više korisnika i uređaja u datom području. - Poboljšana pouzdanost: 5G mreže su izgrađene da budu pouzdanije od 4G mreža, što može pomoći da se minimizira vrijeme zastoja i poboljša ukupni kontinuitet poslovanja.	- Trošak: Troškovi postavljanja i održavanja 5G mreža mogu biti veći od 4G mreža. - Nedostatak pokrivenosti: 5G mreže imaju ograničenu pokrivenost u poređenju sa 4G mrežama, što može ograničiti dostupnost mreže u određenim područjima. - Smetnje: 5G mreže mogu imati više smetnji od 4G mreža zbog viših frekvencijskih opsega koji se koriste. - Implementacija: Postavljanje 5G mreža može biti složeno i dugotrajno.

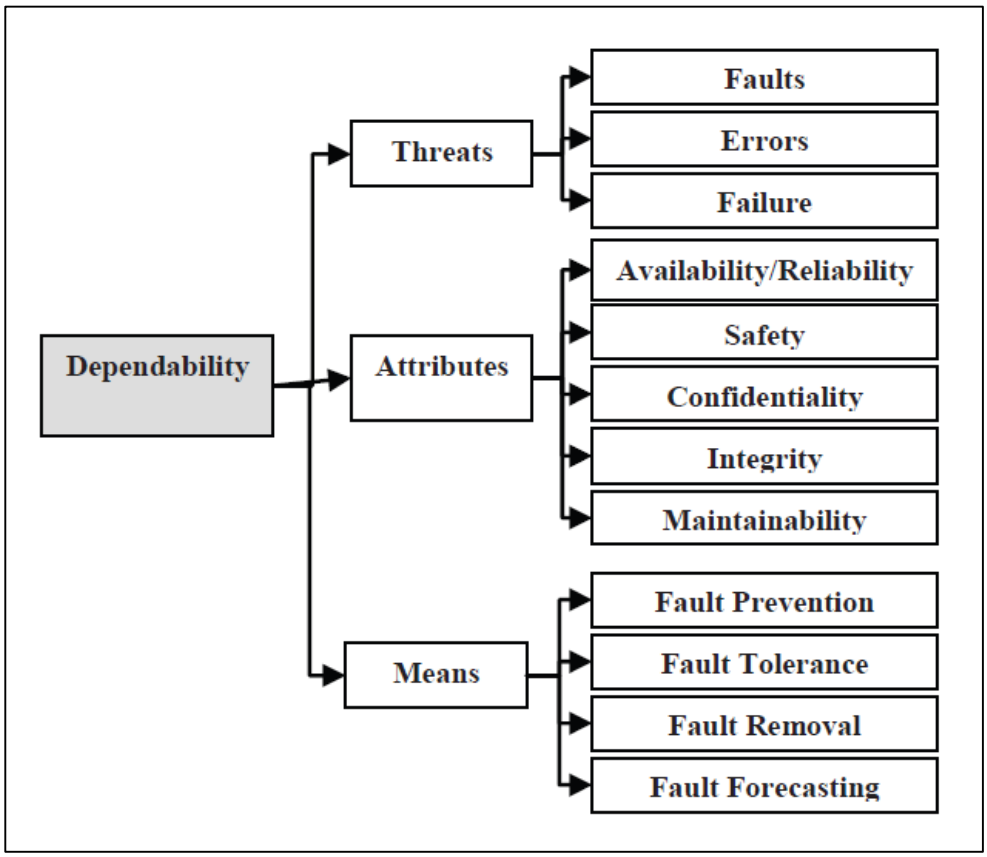
Izvori: Ahmed, Haskell-Dowland (2021); Marcham (2021); Bai, Scholl (2021); Yang et al. (2021); Buyya (2019); Al-Turjman (2019); Taheribakhsh et al. (2020)

3.8. Komparacija koncepata kontinuiranog kompjutinga

U prethodnim poglavljima detaljno su istraženi različiti aspekti tehnologija za kontinuirani kompjuting kroz komparativnu analizu prednosti i nedostataka svake tehnologije. Ove komparacije omogućile su nam da sagledamo širu sliku tehnološkog opsega kontinuiranog kompjutinga, ističući kako različite tehnologije mogu zadovoljiti različite zahtjeve korisnika. Da bi se ispravno odgovorilo na te zahtjeve, pri odabiru tehnologije za kontinuirani kompjuting potrebno je uzeti u obzir više faktora, uključujući i kontekst primjene, specifične potrebe korisnika i potencijalne rizike. Komparativnom analizom ovih tehnologija mogu se identifikovati ključni koncepti kontinuiranog kompjutinga koji su i predstavljeni u članku „A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability“ (Al-Kuwaiti, Kyriakopoulos, Hussein, 2009):

a) „Dependability“ (pouzdanost): kao što to autori navode, ne postoji precizna definicija za *dependability*. Moglo bi se definisati kao sposobnost sistema da omogući specifične usluge kojima se može „opravdano ili pouzdano vjerovati“. U kontekstu kontinuiranog kompjutinga, ovo znači da se korisnici mogu osloniti na sistem, da će biti dostupan i funkcionisati kada je to potrebno. Generalizovani prikaz karakteristika koncepta *Dependability* se nalazi na slici 1:

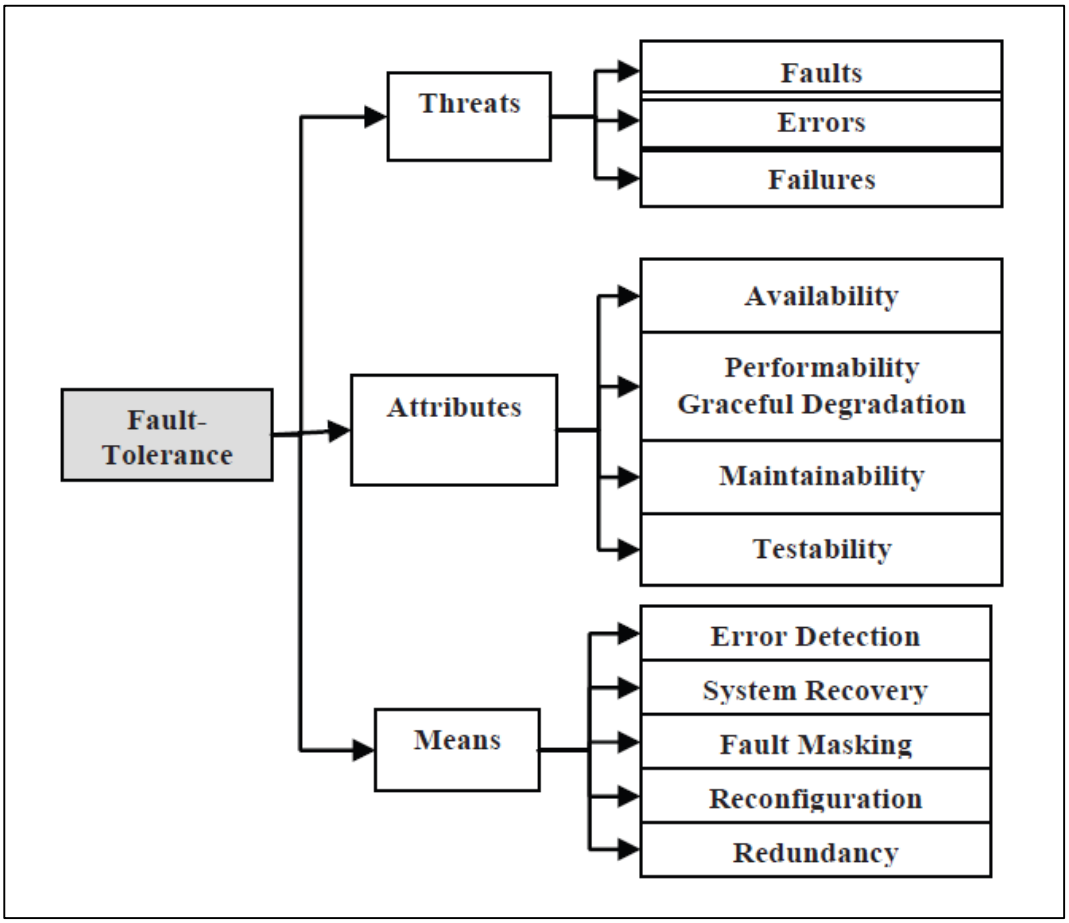
Slika 1. Taksonomija koncepta "Dependability"



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

b) „Fault-Tolerance“ (otpornost na kvarove, tolerancija kvarova): predstavlja sposobnost sistema ili dijelova sistema da nastave s normalnim radom iako se dogodi hardverska ili softverska greška. Sistem otporan na greške je sistem koji ima mogućnost da nastavi ispravno izvršavanje aplikacija i procesiranje ulaznih i izlaznih podataka ako se i desi neka sistemska greška. Ovo osigurava neprekidnost usluge i minimalno ometanje za korisnike. Na slici 2 se nalazi taksonomija koncepta *Fault-Tolerance*:

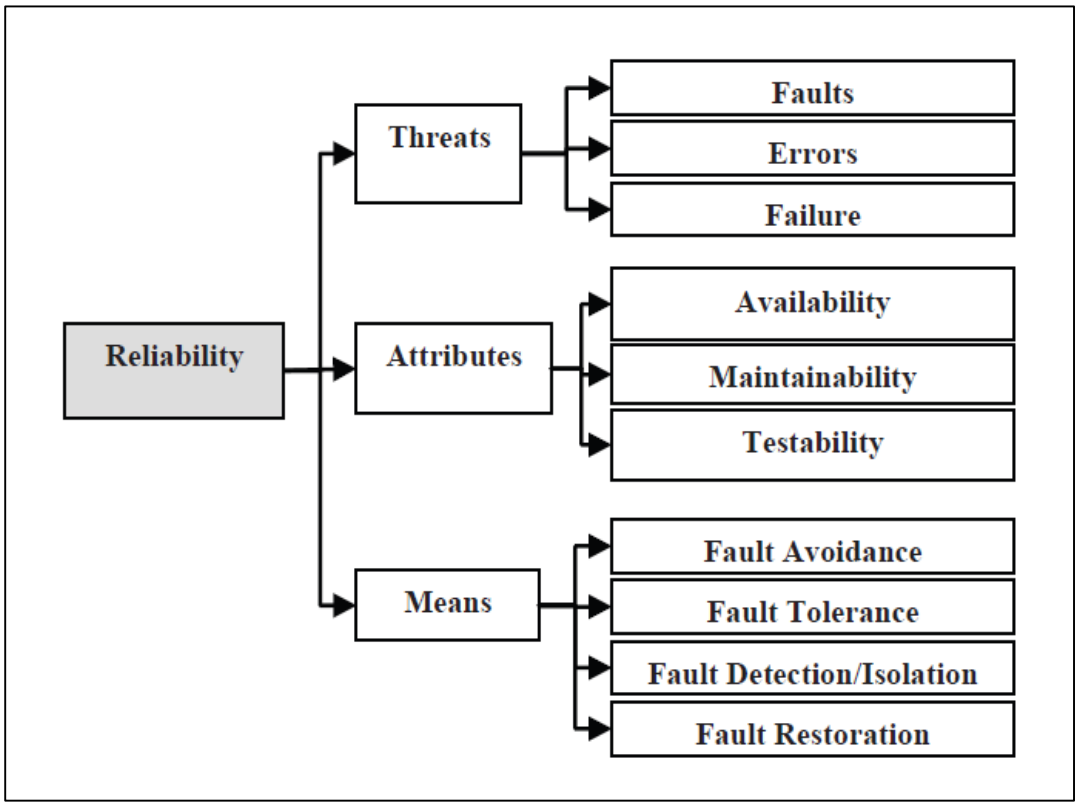
Slika 2. Taksonomija koncepta "Fault-Tolerance"



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

c) *„Reliability"* (pouzdanost, robusnost): za razliku od koncepata *dependability* i *fault-tolerance,* koncept *reliability* je egzaktno mjerljiv i može biti prikazan kroz preciznu matematičku funkciju. Definiše se kao sposobnost sistema ili dijela sistema da izvrši tražene zahtjeve ili operacije u postavljenim uvjetima i vremenskom razdoblju. U kontinuiranom kompjutingu, pouzdanost je od ključnog značaja jer korisnici trebaju biti sigurni da će sistem biti dostupan kada ga trebaju koristiti. Generalizovani prikaz karakteristika koncepta *reliability* se nalazi na slici 3:

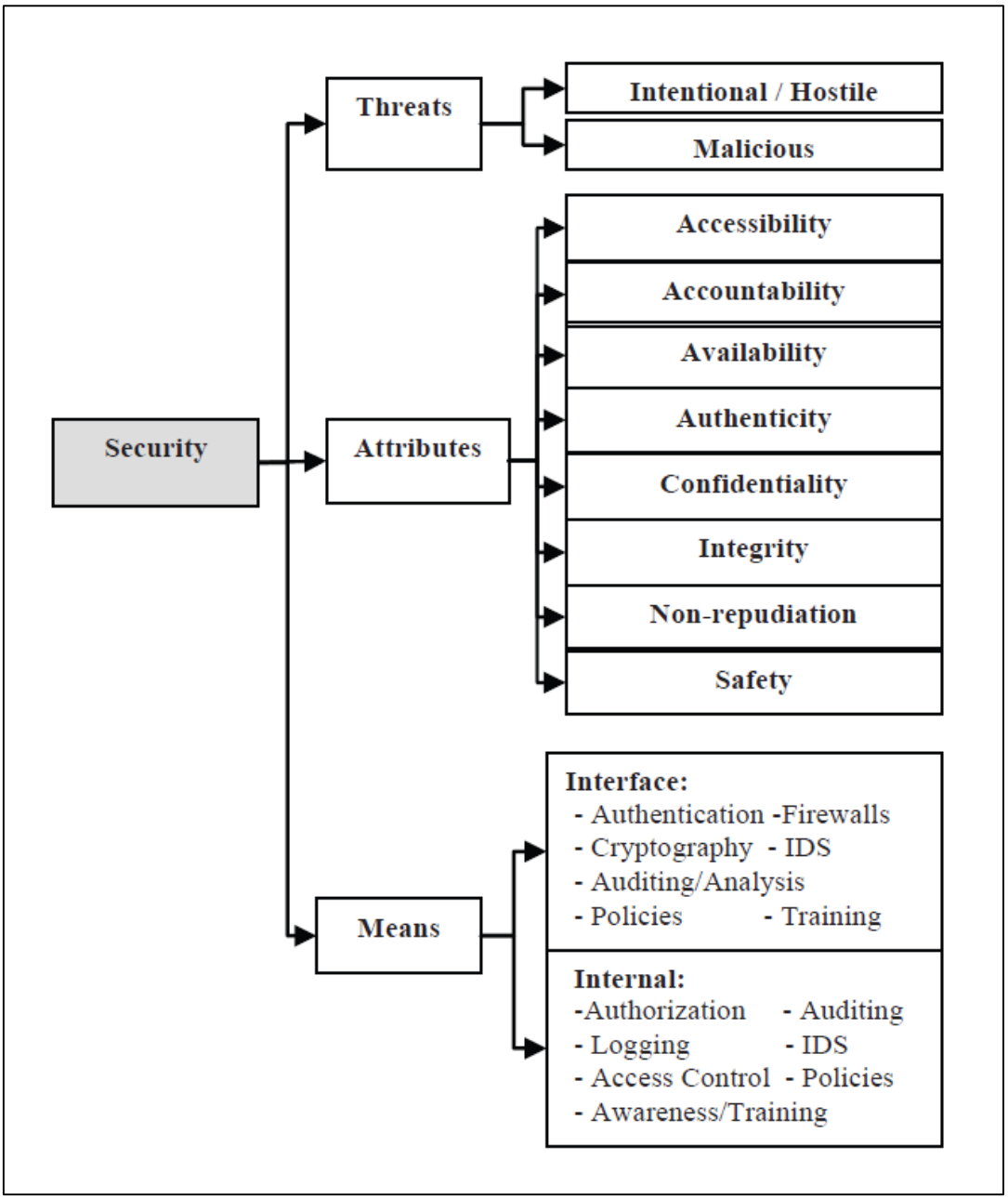
Slika 3. Taksonomija koncepta "Reliability"



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

d) *„Security"* (sigurnost, zaštićenost): u širem smislu predstavlja zaštitu od neželjenih događaja ili akcija. U kontekstu IT tehnologija to može predstavljati neovlašteni pristup, zloupotrebu podataka ili napad na sistem. Sigurnosni propusti mogu dovesti do prekida usluge ili gubitka podataka, što može biti neprihvatljivo u kontekstu kontinuiranog kompjutinga. Na slici 4 se nalazi taksonomija koncepta *Security*:

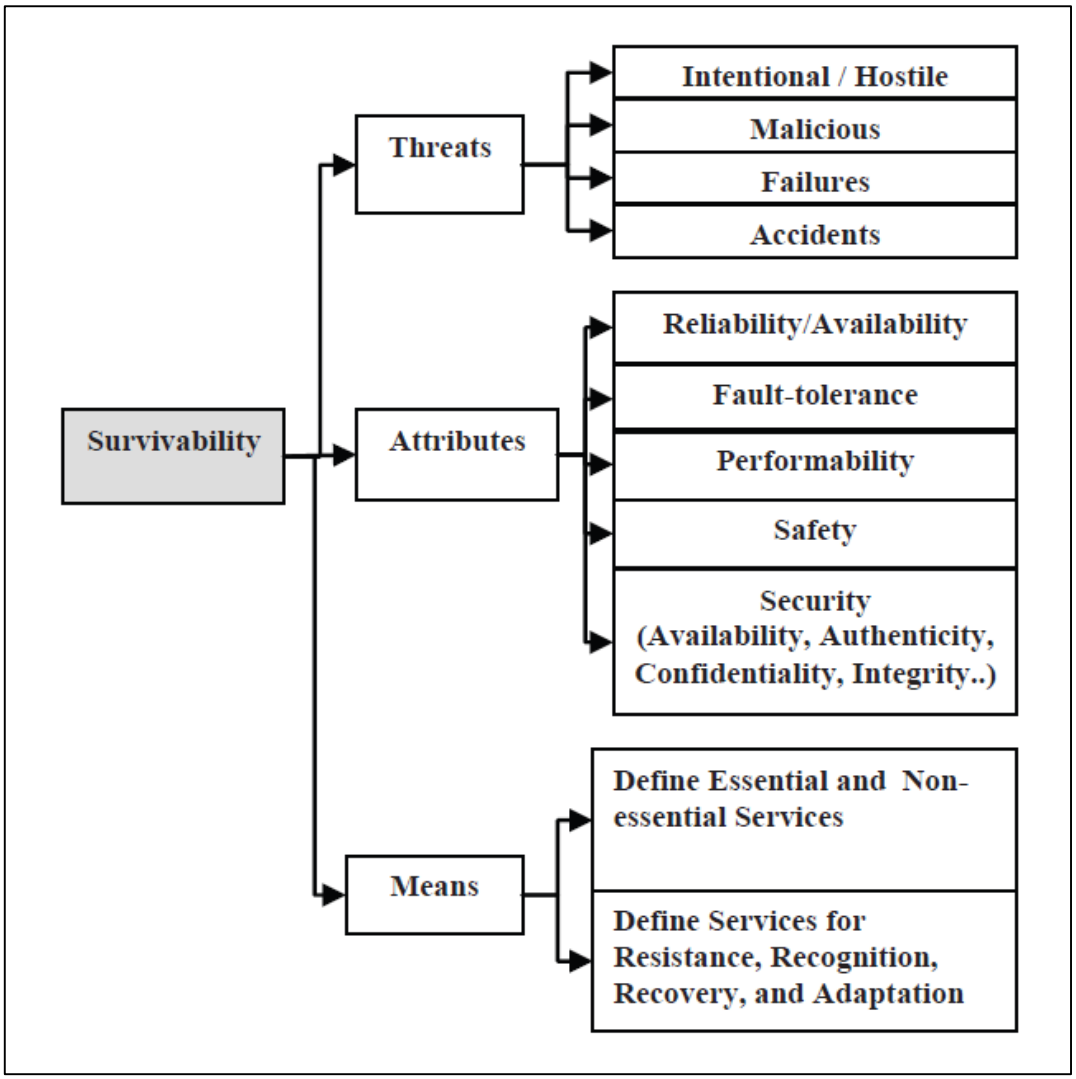
Slika 4. Taksonomija koncepta "Security"



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

e) *„Survivability"* (otpornost, sposobnost opstanka): prema autorima, ovaj koncept predstavlja sposobnost sistema da izvršava svoju funkcionalnost u zadanom vremenu u prisustvu kvarova, napada ili katastrofe. Otporan sistem mora prvi reagovati i pokušati oporaviti funkcionalnost od učinjene štete prije nego što se desi potpuno gašenje ili rušenje sistema. Dakle, u trenucima ugroženosti, sistem mora raditi s manjim brojem funkcionalnosti ili raditi dovoljno dugo kako bi obavio ključne procese prije potpunog gašenja. U kontekstu kontinuiranog sistem mora preživjeti različite vrste incidenata ili nepovoljnih situacija i nastaviti pružati uslugu bez većih prekida. Na slici 5 se nalazi taksonomija koncepta *Survivability*:

Slika 5. Taksonomija koncepta "Survivability"



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

Autori navode kako je za dublju analizu ovih pet koncepata potrebno identifikovati i komparirati metode, indikatore i metrike performansa svakog koncepta. U tabeli 12 se nalaze sve metode koje su autori predstavili:

Tabela 12. Komparacija metoda mjerenja performansa

Naziv koncepta	Metoda mjerenja performansa
Reliability	• Reliability, R(t), Unreliability, Q(t) • Availability, A(t), and Unavailability, U(t) • Mean Time Between Failure (MTBF) • Mean Time To Failure (MTTF) • Mean Time To Repair (MTTR) • Failure Rate (λ) • Repair Rate or Maintainability Parameter (μ)

Fault-Tolerance	• Maximum allowable failure rate (λ), repair rate (μ), MTBF, MTTF, and MTTR • Fault-coverage (mjera sposobnosti sistema da detektuje, locira, zaustavi grešku i oporavi se od iste.
Security	• Mjerenje sigurnosti sistema prema modelu povjerljivosti, „Bell-LaPadula" model. • Mjerenje sigurnosti sistema prema modelu integriteta, „Biba" model. • Mjerenje sigurnosti sistema prema modelu povjerljivosti i integriteta, „Chinese Wall" model. • Model mjerenja sigurnosti naspram rizika od učestalosti kvarova, prijetnji, ranjivosti, trajanja prekida rada itd. Formula za računanje rizika, ρ, je: $\rho = T \times V \times C$, gdje je T prijetnja ili učestalost problema, izraženo u procentima, V je ranjivost ili vjerovatnoća da će prijetnja imati utjecaj na sistem, i C je trošak ili šteta prouzrokovana prijetnjom. • Jedan od najčešće korištenih sigurnosnih evaluacijskih dokumenata TCSEC (engl. *US Trusted Computer System Evaluation Criteria*).
Dependability	• Alati i modeli za mjerenje: SAVE, SHARPE, UltraSAN and MEADEP
Survivability	• Statistički modeli koji koriste parametre: MTTF, MTTR, MTBF, Failure Rate (λ), Repair Rate or Maintainability Parameter (μ), Fault-coverage. • Given Occurrence of Failure (GOF) model • Occurrence of Failure (ROF) model • Continuous Time Markov Chain (CTMC) model.

Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

3.8.1. Komparacija koncepata

U svom radu, autori Al-Kuwaiti, Kyriakopoulos, Hussein (2009) navode da su neki od ovih koncepata prisutni već od početka razvoja određene tehnološke oblasti. Za primjer se može uzeti oblast poput dizajna sistema, jer su koncepti pouzdanosti (engl. *reliability*) i tolerancije na greške (engl. *fault-tolerance*) duboko ukorijenjeni u njihovim funkcionalnostima. Dok su drugi koncepti noviji i razvijali su se zajedno s tehnologijom, poput pouzdanosti (engl. *dependability*) i otpornosti (engl. *survivability*).

Raščlanjivanje ovih koncepata, kao što su pouzdanost (engl. *dependability*) i otpornost (engl. *survivability*) na njihove specifične atribute, a to su pouzdanost (engl. *reliability*) i dostupnost (engl. *availability*), nužno je kako bi se steklo bolje razumijevanje koncepata. Upravo ovom dekompozicijom koncepata na jednostavnije i objektivnije atribute, možemo formirati kvantitativne i kvalitativne karakteristike ovih koncepata. U tabeli 13 se nalazi

komparativna analiza koncepata raščlanjena na njihove definicije, ciljeve, funkcionalnosti, atribute, prijetnje i načine mjerenja.

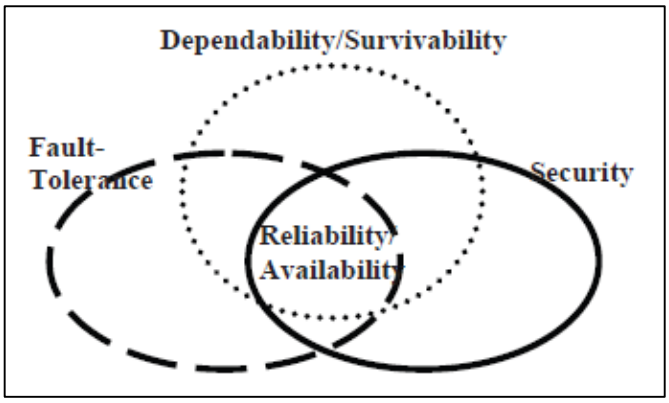
Tabela 13. Komparacija koncepata

	Dependability	Fault-Tolerance	Reliability	Security	Survivability
Definition and Goal	An umbrella concept defined as the ability to deliver required services during its life cycle that can justifiably be trusted	Ability to continue the performance of its tasks in the presence of faults	A conditional probability that a system performs its intended tasks correctly throughout a complete interval of time	Ability to guard and protect from unwanted happenings or actions and preserve confidentiality, integrity, and availability	Ability to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents
Means	- Fault-prevention - Fault tolerance - Fault removal - Fault forecasting	- Error detection - System recovery - Fault masking - Reconfiguration - Redundancy	- Fault avoidance - Fault tolerance - Fault detection and isolation - Fault Restoration	- Interface: IDS, cryptography, auditing, analysis, firewalls, authentication. - Internal: IDS, access control, authorization, auditing/logging, - Policies - Awareness and training	- Define essential and nonessential services - Define survivability services for attack resistance, recognition, and recovery.
Attributes	- Availability - Confidentiality - Integrity - Maintainability - Reliability - Safety - Security	- Availability - Maintainability - Performability/ Graceful Degradation - Testability	- Availability - Maintainability - Testability	- Accessibility - Accountability - Authenticity - Availability - Confidentiality - Integrity - Non-repudiation - Awareness and - Safety	- Availability - Fault-tolerance - Performability - Reliability - Safety - Security (confidentiality, integrity, availability, authenticity)
Cause of Threats and Evaluation Criteria	- Errors, faults, failures - Caused by random, accidental, and unintentional events in hardware or rare events in software, and this randomness can be quantified or modeled	- Errors, faults, failures - Caused by random, accidental, and unintentional events in hardware or rare events in software, and this randomness can be quantified or modeled	- Errors, faults, failures - Caused by random, accidental, and unintentional events in hardware or rare events in software, and this randomness can be quantified or modeled	- Intentional and hostile - Malicious - Failures are caused by human intent, resulting in security failures which are hard to model	- Intentional attacks, failure, and accidents include all potential damaging events - Randomness can be assumed for accidental faults, but not for attacks

Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

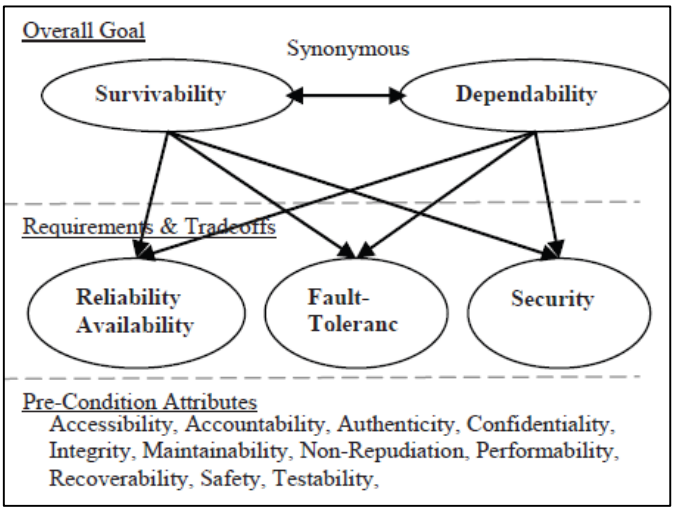
Ovisno o kontekstu u kojem se koriste, pojmovi ili koncepti mogu imati različita značenja. Pregled tabele 13 naglašava da navedeni koncepti imaju zajedničke karakteristike te da se u njihovoj upotrebi i funkcionalnosti može primijetiti određeno preklapanje. Iako su u određenoj mjeri konceptualno slični, kada se usporede međusobno, ovi pojmovi nisu u potpunosti različiti niti identični. Slike 6 i 7 pružaju detaljan pregled njihovih međusobnih odnosa, što pomaže u boljem razumijevanju njihove dinamike i konteksta.

Slika 6. Odnos između koncepata



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

Slika 7. Hijerarhija i međuzavisnost koncepata



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

Kada su u pitanju koncepti *dependability* i *survivability*, a uzimajući u obzir podatke iz tabele 13 i slike 6, autor zaključuje da se, po svojim ciljevima i atributima, ovi koncepti znatno preklapaju. Koncept *survivability* pridaje veću pažnju zlonamjernim vrstama prijetnji budući da je evoluirao u svrhu rješavanja sigurnosnih problema. Uz to, važno je napomenuti da su koncepti *reliability* i *availability* među najčešće korištenim objektivnim atributima kod svih pet koncepata koje obrađuje ova analiza. Njihova dugotrajna prisutnost i široka primjena doprinose njihovoj centralnoj ulozi u ovim konceptima. Da bismo se adekvatno nosili s izazovima povezanim s kompleksnim infrastrukturama poput IT infrastrukture, potrebno je inkorporirati *reliability* i *availability* koncepte, uz dodatak odgovarajućeg segmenata i funkcionalnosti *fault-tolerance* koncepta. Ključni atribut *fault-tolerance* koncepta koji je od suštinske važnosti jeste zapravo kontinuirani performans, tj. rad bez prekida. To podrazumijeva sposobnost održavanja funkcionalnosti sistema u situacijama degradirane performanse. Kada je u pitanju sigurnost, omogućavanje pristupačnosti, autentičnosti i

integriteta je ključno. Osiguravanjem ovih karakteristika omogućuje se efikasno upravljanje rizicima i održavanje integriteta infrastrukture u dinamičnom okruženju.

Iako postoji određena sličnost ili paralelizam među ovim konceptima, kako to autori navode, također se može primijetiti i određen nivo hijerarhije prikazan na slici 7. Koncepti *dependability* i *survivability* mogu se pozicionirati na najviši nivo, dok se svi ostali koncepti i njihovi odgovarajući kvalitativni i kvantitativni atributi mogu sagledati kao dodatni zahtjevi koji pružaju podršku cjelokupnom sistemu. Ova hijerarhijska struktura omogućava sistematičan pristup razumijevanju složenosti i zahtjeva sistema, omogućavajući efikasnije planiranje i implementaciju infrastrukture.

Neke od atributa koncepta iz tabele 13 možemo smatrati kvalitativnim, dok se drugi mogu smatrati kvantitativnim. U svom radu, autori su predstavili tabelu 14, koja prikazuje popis ovih atributa, zajedno s naznakom jesu li oni mjerljivi ili ne. Ova komparacija atributa omogućuje detaljnije razumijevanje svakog koncepta pojedinačno i pruža osnovu za odgovarajuće analize. Identifikacija mjerljivih atributa olakšava kvantifikaciju performansi i čini temelj za donošenje odluka u procesu dizajniranja i upravljanja sistemima.

Tabela 14. Komparacija mjerljivosti atributa koncepata

Concept Attributes		Measurability	
No.	Attributes	Measurable	Immeasurable
1	Accessibility		x
2	Accountability		x
3	Authenticity		x
4	Availability	x	
5	Confidentiality		x
6	Fault-Tolerance	x	
7	Integrity	x	
8	Maintainability	x	
9	Non-Repudiation		x
10	Performability	x	
11	Reliability	x	
12	Safety		x
13	Security		x
14	Testability		x
15	Unreliability	x	
16	Unavailability	x	

Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

Nakon detaljnijeg pregleda podataka u tabeli 14, postaje očigledno da su mjerljivi atributi zapravo oni koji se češće povezuju s proučavanim konceptima. Ti mjerljivi atributi uključuju dostupnost (engl. *availability*), otpornost na greške (engl. *fault-tolerance*), održivost (engl. *maintainability*) i pouzdanost (engl. *reliability*). Kako autori navode, što su više mjerljivi atributi prisutni u konceptu, lakše je procijeniti utjecaj tog koncepta i uskladiti ga s drugim

atributima. Ovi mjerljivi elementi pružaju kvantitativne podatke koji omogućuju preciznije analize i donošenje odluka, poboljšavajući tako razumijevanje performansi sistema i omogućujući efikasnije upravljanje njihovim resursima.

Mjerljivi atributi su, ustvari, blisko povezani s određenim mjerljivim parametrima koji omogućuju procjenu stvarnog performansa tog atributa. Analiza različitih metoda mjerenja pet koncepata rezultirala je identifikacijom nekoliko mjerljivih parametara koji su povezani s tim atributima. Autori su definisali sljedeću tabelu 15, u kojoj se nalazi lista ovih parametara za mjerljive atribute.

Tabela 15. Komparacija parametara

SET OF QUANTIFIABLE PARAMETERS FOR THE COMMON ATTRIBUTES.

Reliability / Fault Tolerance	Availability / Maintainability
MTTF	Steady State Availability, A_{ss}
Reliability Function, $R(t)$	Unavailability, U
Failure Rate Function, $z(t)$	MTBF
Unreliability Function, Q(t)	MTTR
Failure Rate (λ)	Repair Rate (μ)
Fault Coverage	

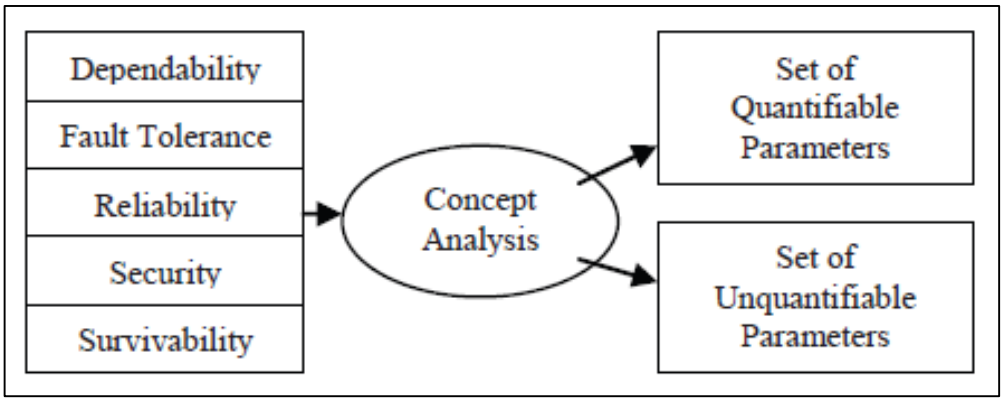
Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

Autori Al-Kuwaiti, Kyriakopoulos, Hussein (2009) istaknuli su da se u nekim kontekstima koriste različiti termini koji se odnose na slične parametre. Naprimjer, izrazi poput MTTR, MTBF i stopa popravaka (engl. *repair rate*) kod koncepta *survivability* često podrazumijevaju analizu obnovljivosti (engl. *restorability),* dok se kod koncepta *reliability* ti parametri koriste za mjerenje održivosti sistema. Modeliranje koncepta *fault-tolerance* uključuje korištenje parametara koji su povezani s modeliranjem pouzdanosti, poput MTTF, stope kvarova (λ), funkcije pouzdanosti R(t) i stope grešaka z(t). Ova terminološka varijacija može izazvati konfuziju, ali razumijevanje da se pojedini pojmovi mogu koristiti s različitim konotacijama u različitim kontekstima ključno je za jasnoću i preciznost razumijevanja ovih koncepata.

Pouzdanost (engl. *reliability*) i dostupnost (engl. *availability*) imaju najbolji opseg mjerljivosti parametrima, koji služe kao pokazatelji performansa. Ti parametri igraju ključnu ulogu pri optimizaciji dizajna i ostvarivanju postavljenih ciljeva funkcionisanja sistema. Važno je naglasiti da bez dostupnosti (engl. *availability*), nijedan od ovih koncepata ne bi mogao funkcionisati, jer je nedostupan sistem isto što i nepostojeći. Budući da su svi sistemi podložni kvarovima, neophodne su metode za modeliranje i mjerenje njihove pouzdanosti i dostupnosti. Shodno tome, postoji velika potreba za razvojem alata i procedura za analiziranje pouzdanosti i dostupnosti.

Rezultati korištenja komparativne metodologije koju su autori prezentovali u ovom naučnom članku pokazuju da mjerenje performansa kompleksnih infrastruktura iziskuje upotrebu dvije komplementarne metode evaluacije – kvalitativne i kvantitativne. Autori su to predstavili i grafički, slika 8.

Slika 8. Metoda evaluacije koncepata



Izvor: Al-Kuwaiti, Kyriakopoulos, Hussein, (2009)

Kako bi se postigao optimalan dizajn sistema, tj. ispravno izmjerio performans, potrebno je koristiti oba pristupa. Glavni razlog jeste da čista kvantitativna ili kvalitativna procjena možda neće potpuno obuhvatiti sve različite aspekte ovih koncepata. Tako da ova dva pristupa ili metode možemo grupisati u (Al-Kuwaiti, Kyriakopoulos, Hussein, 2009):

a) Skup parametara koji nisu mjerljivi: predstavljaju parametre koji mogu imati utjecaj na dizajn sistema ili služe kao preventivne mjere, a sve u svrhu povećanja otpornosti sistema na greške, razne prijetnje, prestanak rada i slično. Ovaj tip parametara se često primjenjuje u kontekstu sigurnosnih rizika jer nema mjerljivih metrika evaluacija. Primjeri takvih parametara uključuju metode analize rizika, sisteme za otkrivanje upada, sigurnosne mehanizme, upravljanje pravilima itd. Raznolikost ovih nemjerljivih parametara pruža širok spektar alata i strategija za unapređenje sigurnosti sistema, omogućujući prilagodljiv pristup različitim sigurnosnim izazovima.

b) Skup mjerljivih parametara: predstavljaju parametre koji mogu biti uključeni u početne karakteristike dizajna sistema i zahtjeva. Ti parametri se mogu ugraditi u sistem u svrhu kontrole. Integracija ovih parametara u dizajna sistema omogućuje inžinjerima da postave jasne ciljeve i standarde te ih prilagode zahtjevima specifičnog okruženja ili industrije. Oni se bave različitim aspektima sistema, kao što su vjerovatnost kvara, pouzdanost i dostupnost sistema. Kroz praćenje i kontrolu ovih parametara, moguće je ostvariti bolje razumijevanje i upravljanje performansama sistema te unaprijediti njegovu efikasnost i pouzdanost.

Kao zaključak ovog poglavlja možemo reći da su autori (Al-Kuwaiti, Kyriakopoulos, Hussein, 2009) u ovom naučnom članku predstavili detaljnu komparativnu analizu pet široko korištenih koncepata: pouzdanost (engl. *dependability*), tolerancija na greške (engl. *fault-tolerance*), pouzdanost (engl. *reliability*), sigurnost (engl. *security*) i preživljavanje (engl. *survivability*). Kroz sistematičan metodološki pristup urađena je komparacija definicija, atributa, metoda mjerenja i parametara, koja je prikazana tabelarno. Ova analiza pomaže u mapiranju općih korisničkih zahtjeva na objektivne parametre performansi, što olakšava analizu i dizajn informacijskih infrastruktura. Rezultat analize je i komparacija metoda mjerenja koncepata iz koje su izvučeni i grupisani parametri tih metoda. Komparativna analiza navedenih pet koncepata jasno ističe njihovu nezamjenjivu ulogu u održavanju kontinuiteta poslovanja. Integracija ovih koncepata u dizajn informacionih sistema pruža temelje za izgradnju otpornih i pouzdanih infrastruktura, ključnih za suočavanje s izazovima nepredviđenih situacija i osiguranje kontinuiranog funkcionisanja poslovnih procesa. Razumijevanje specifičnih karakteristika svakog pojedinog koncepta i njihova uspješna primjena u stvarnim poslovnim scenarijima su vitalni za osiguranje stabilnosti i uspješnosti poslovanja u današnjem dinamičnom poslovnom okruženju.

4. ZAKLJUČAK

Uvodni dio rada postavlja temelje za istraživanje, identifikujući predmet i problem istraživanja. Uz to, definiše svrhu i ciljeve ovog istraživanja, s naglaskom na važnost razumijevanja kontinuiteta poslovanja u današnjem, tehnološki naprednom i dinamičnom poslovnom okruženju. Također, prezentovane su metodologija istraživanja i cjelokupna struktura rada.

U sklopu drugog dijela rada, detaljno su proučeni koncepti kontinuiteta poslovanja i kontinuiranog kompjutinga. Kroz sistemski pregled literature i istraživanja, pojašnjena su značenja i bitne karakteristike ovih pojmova, što uključuje važnost kontinuiteta poslovanja u sprečavanju i upravljanju rizicima te osiguravanje stabilnosti organizacije u slučaju neočekivanih događaja. U ovom dijelu rada također je dat historijski osvrt razvoja kontinuiteta poslovanja i kontinuiranog kompjutinga, kako bismo stekli bolji uvid u evoluciju ovih disciplina i razumjeli kako su se prilagođavale tehnološkim promjenama tokom vremena.

Posebna pažnja, također u drugom dijelu rada, posvećena je upravljanju kontinuitetom poslovanja i njegovom planiranju. Predstavljene su različite strategije, pristupi i najbolje prakse upravljanja kontinuitetom poslovanja. Također, istražena je tematika oporavka od katastrofe, što uključuje planiranje i implementaciju procedura za brz oporavak te tehnike oporavka i rješenja koje osiguravaju minimalno vrijeme nedostupnosti usluga i povratak u normalno stanje. U kontekstu upravljanja rizicima u poslovanju, predstavljena je važnost upravljanja, identifikacije i procjene rizika, koji mogu utjecati na kontinuitet poslovanja.

Treći dio rada posvećen je i fokusiran na implementaciju tehnologija za kontinuirani kompjuting (engl. *continuous computing*) te njihovo poređenje kroz dvije komparativne analize. Cilj je pružiti uvid u različite aspekte implementacije ovih tehnologija, s fokusom na server računare, server operativne sisteme, baze podataka, tehnologije za *backup* podataka, računarske mreže, *cyber*-sigurnost, *cloud computing* i virtualizaciju, kao i na druge nove tehnologije koje mogu biti relevantne za kontinuitet poslovanja.

Može se istaknuti da server računari, kao centralni element kontinuiranog kompjutinga, moraju biti opremljeni pouzdanim hardverom i efikasnim mehanizmima za obnovu sistema kako bi osigurali neprekidan rad i minimizirali rizik od prekida usluga. Server računari uz server operativne sisteme igraju ključnu ulogu u pružanju stabilnog okruženja za aplikacije i servise, što zahtijeva adekvatno upravljanje resursima i optimizaciju performansa.

Baze podataka i tehnologije za *backup* podataka su od vitalnog značaja za osiguranje cjelovitosti i zaštite podataka od gubitka ili oštećenja. Pravilno konfigurisanje i sigurnosno zaštićene baze podataka omogućavaju brz oporavak u slučaju kvara i sprečavaju gubitak vrijednih informacija.

U kontekstu računarskih mreža, kontinuirani kompjuting zahtijeva visoku dostupnost i pouzdanost komunikacijskih kanala između sistema. Pravilna konfiguracija mrežne infrastrukture i redundancija ključnih komponenata, omogućavaju održavanje kontinuiteta poslovanja, čak i u slučaju otkazivanja pojedinih elemenata.

Prilikom razmatranja *cyber*-sigurnosti, iako ona ne spada u klasičnu tehnologiju za kontinuirani kompjuting, možemo uvidjeti da su informacioni sistemi podložni raznim sigurnosnim prijetnjama i napadima. Stoga, važno je implementirati sofisticirane sigurnosne mehanizme i sisteme za zaštitu od *cyber* prijetnji kako bi se osigurali integritet, povjerljivost i dostupnost podataka i infrastrukture.

Cloud computing i virtualizacija su ključni elementi koji omogućavaju fleksibilnost, skalabilnost i efikasno korištenje resursa, doprinoseći time kontinuitetu poslovanja. Međutim, pravilno planiranje i upravljanje virtualnim okruženjima je ključno kako bi se osigurala optimalna izvedba i izbjegle potencijalne slabosti koje mogu utjecati na kontinuitet rada.

Ostale nove tehnologije navedene u ovom radu možda ne možemo direktno svrstati u klasične ili primarne tehnologije za kontinuirani kompjuting, ali možemo zaključiti da one imaju veliki potencijal i mogu biti korisne u osnaživanju postojećih tehnologija za kontinuirani kompjuting.

U trećem dijelu rada su predstavljene dvije komparativne analize. Prva analiza predstavlja komparativnu analizu različitih tehnologija za kontinuirani kompjuting, koja se temelji na eksploraciji prikupljenih relevantnih informacija o prednostima i nedostacima svake tehnologije, identifikujući zajedničke karakteristike i obrasce među njima. Komparativna

analiza u ovom slučaju nije bazirana na kvantitativnim numeričkim i statističkim podacima, već na općoj slici prednosti i nedostataka tehnologija kontinuiranog kompjutinga u kontekstu performanse, energetske efikasnosti, pouzdanosti, sigurnosti, kompleksnosti, skalabilnosti i fleksibilnosti svake tehnologije. Rezultat ove analize prikazan je tabelarno kroz prednosti i nedostatke tehnologija za kontinuirani kompjuting. Kao zaključak ove analize, možemo reći da nema univerzalnog pristupa za implementaciju tehnologija za kontinuirani kompjuting. Komparativna analiza pokazuje da je važno prilagoditi odabir tehnologija specifičnim potrebama i zahtjevima organizacije te karakteristikama domene u kojoj će se primjenjivati.

Druga komparativna analiza bazirana je na analizi pet ključnih koncepata kontinuiranog kompjutinga: pouzdanost (engl. *dependability*), tolerancija na kvarove (engl. *fault-tolerance*), pouzdanost (engl. *reliability*), sigurnost (engl. *security*) i otpornost (engl. *survivability*). Kroz sistematičan metodološki pristup prikazana je komparacija definicija, atributa, metoda mjerenja i parametara ovih koncepata. Rezultat analize je i komparacija metoda mjerenja koncepata iz koje su izvučeni i grupisani parametri tih metoda. Ova analiza pokazuje da su navedeni koncepti inherentno povezani s tehnologijama za kontinuirani kompjuting jer su ključne za osiguravanje stabilnosti, sigurnosti i pouzdanosti sistema koji moraju neprekidno pružati usluge i raditi u izazovnim okruženjima. Integracija ovih koncepata u dizajn i implementaciju tehnologija za kontinuirani kompjuting ključna je za postizanje visoke razine performansi i uspjeha u operativnim zadacima.

Finalna svrha ovog rada jeste ispitivanja glavne H1 hipoteze koja je postavljena na početku. Kroz detaljnu kvalitativnu i teoretsku analizu prikupljenih podataka i informacija iz relevantnih literatura, istraživačkih radova i relevantnih studija slučaja, te uzimajući u obzir rezultate obje komparativne analize, istraživanje potvrđuje glavnu hipotezu. Dakle, implementacija tehnologije za kontinuirani kompjuting ima pozitivan utjecaj na kontinuitet poslovanja kompanija.

Nadam se da će ovaj rad doprinijeti daljnjem istraživanju, razvoju i primjeni tehnologija za kontinuirani kompjuting, te da će pružiti smjernice za odabir odgovarajućih tehnologija i pristupa, uzimajući u obzir specifične zahtjeve domene. Iako su u ovom istraživanju identifikovani najvažniji aspekti implementacije tehnologija za kontinuirani kompjuting, treba naglasiti da se ova oblast brzo razvija. Stalni napredak tehnologije donosi nove izazove i mogućnosti, a s njima se pojavljuju i nova istraživanja. Preporučuje se daljnje istraživanje novih tehnologija kako bi se bolje razumjeli najnoviji trendovi i potencijali u kontinuiranom kompjutingu, te identifikovale najbolje prakse za njihovu implementaciju.

REFERENCE

1. Adekotujo, A., Odumabo, A., Adedokun, A., Aiyeniko, O. (2020). A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS. *International Journal of Computer Applications*. 176. 16-23.
2. Ahmed, M., Haskell-Dowland, P. (2021). *Secure Edge Computing: Applications, Techniques and Challenges*. CRC Press.
3. Al-Ali, J., Nasir, Q., Dweiri, F., T., (2019). Business Continuity Management Framework of Internet of Things (IoT). *Advances in Science and Engineering Technology International Conferences (ASET).*
4. AlJahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., Xu, J. (2014). Multi-Tenancy in Cloud Computing. *IEEE 8th International Symposium on Service Oriented System Engineering.*
5. Al-Kuwaiti, M., Kyriakopoulos, N., Hussein, S. (2009). A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability. *IEEE communications surveys & tutorials*, VOL. 11, NO. 2
6. Altheide, C., Carvey, H. (2011). *Digital Forensics with Open Source Tools*. Elsevier Inc.
7. Al-Turjman, F. (2019). *Edge Computing: From Hype to Reality*. Springer
8. Andrade, E., Nogueira, B., Matos, R., Callou, G., Maciel, P. (2017). *Availability modeling and analysis of a disaster-recovery-as-a-service solution*. Springer-Verlag.
9. Anis Aziz, W., Babulak, E., & Al-Dabass, D. (2021). *Network Function Virtualization over Cloud-Cloud Computing as Business Continuity Solution*. Digital Service Platforms. IntechOpen, Nov. 17, 2021
10. Anton, E., Ayesta, U., Jonckheere, M., Verloop, I., M. (2019). *Redundancy with processor sharing servers*. Association for Computing Machinery, New York, USA.
11. Applegate, L. M., Austin, R. D., McFarlan F. W. (2003). *Corporate Information Strategy and Management: The Challenges of Managing in a Network Economy*. New York, SAD: McGraw-Hill
12. Applegate, L. M., Austin, R. D., Soule, D. L. (2009*). Corporate Information Strategy and Management: Text and Cases*. New York, SAD: McGraw-Hill
13. Asnar, Y. i Giorgini, P. (2008). Analyzing Business Continuity through a Multi-layers Model. *Business Process Management*, 5240. pp. 212-227.
14. Awan, M., T., Khan, K. (2022). Linux vs. Windows: A Comparison of Two Widely Used Platforms. *Journal of Computer Science and Technology Studies*, ISSN: 2709-104X
15. Bai, H., Scholl, B. (2021). *Edge Computing and Capability-Oriented Architecture*. CRC Press.
16. Bajgorić, N. (2006). Information technologies for business continuity: an implementation framework. *Information Management & Computer Security*, Vol. 14 Iss 5 pp. 450 – 466.

17. Bajgorić, N. (2008). *Continuous Computing Technologies for Enhancing Business Continuity*. *Information Science Reference*. IGI – Global.
18. Bajgorić, N. (2009). *Always-On Enterprise Information Systems for Business Continuance: Technologies for Reliable and Scalable Operations*. IGI – Global.
19. Bajgorić, N., Somun-Kapetanović, R. Resić, E., Turulja, L. (2019). *Uvod u metodologiju naučnoistraživačkog rada*. Ekonomski fakultet u Sarajevu.
20. Barbosa, F., P., Charão, A., S. (2012). Impact of pay-as-you-go Cloud Platforms on Software Pricing and Development: A Review and Case Study. *ICCSA* 2012, Part IV, LNCS 7336
21. Bauer, E., Adams, R., Eustace, D. (2012). *Beyond Redundancy: How Geographic Redundancy Can Improve Service Availability And Reliability Of Computer-Based Systems.* New Jearsy, SAD: John Wiley & Sons
22. Bowman, R., H., (2008). *Business Continuity Planning for Data Centers and Systems: A Strategic Implementation Guide*. John Wiley & Sons
23. Brooks, C., J., Grow, C., Craig, P., Short, D. (2018). *Cybersecurity Essentials*. John Wiley & Sons.
24. Bryhni, H., Klovning, E., Kure, O. (2000). A comparison of load balancing techniques for scalable Web servers. *IEEE Network,* vol. 14, no. 4, pp. 58-64
25. Buffington, J. (2010). *Data Protection for Virtual Data Centers*. Indianapolis, SAD: Wiley Publishing.
26. Buyya, R. (2019). *Fog and Edge Computing: Principles and Paradigms*. Wiley.
27. Candel, J. (2022). *Implementing DevSecOps with Docker and Kubernetes*. BPB Publications.
28. Cerullo, V. i Cerullo, M. (2004) Business Continuity Planning: A Comprehensive Approach, *Information Systems Management*, 21:3, 70-78
29. Chauhan, N. (2014). *Principles of operating systems*. Oxford University Press.
30. Chen, J., Cheng, W. (2016). Analysis of web traffic based on HTTP protocol. *24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM),* pp. 1-5
31. Chevance, R. (2005). *Server Architectures: Multiprocessors, Clusters, Parallel Systems, Web Servers, Storage Solutions*. Elsevier Science.
32. DaCosta, F. (2013). *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything.* Apress.
33. Dauti, B. (2022). *Windows Server 2022 Administration Fundamentals*. Packt Publishing.
34. Dreibholz, T., Rathgeb, E., P., (2009). *Overview and evaluation of the server redundancy and session failover mechanisms in the reliable server pooling framework.* University of Duisburg-Essen, Institute for Experimental Mathematics.
35. Drewitt, T. (2012). *Everything you want to know about business continuity*. Ely, Cambridgeshire: IT Governance Publishing.
36. Economides, N., Katsamakas, E. (2006). Linux vs. Windows. *The Economics of Open Source Software Development*, 207–218.

37. Elliott, D., Swartz, E., Herbane, B. (2010). *Business continuity management: A crisis management approach*. Routledge.
38. Elmasri, R., Navathe, S., B., (2015). *Fundamentals of Database Systems*. Pearson.
39. Engemann, K., J., Henderson, D., M. (2011). *Business Continuity and Risk Management: Essentials of Organizational Resilience*. Rothstein Publishing.
40. Gardner, K., Harchol-Balter, M., Scheller-Wolf, A., Velednitsky, M., Zbarsky, S. (2017). Redundancy-d: The Power of d Choices for Redundancy. *Operations Research* 65-4.
41. Gkatziouras, E. (2022). *A Developer's Essential Guide to Docker Compose*. Packt Publishing.
42. Guo, Z, Yang, Y. (2014). *Exploring server redundancy in nonblocking multicast data center networks*. IEEE Transactions on Computers.
43. Haber, M., J. (2020). *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*. Apress.
44. Hamadah, S., Aqel, D. (2019). A Proposed Virtual Private Cloud-Based Disaster Recovery Strategy. *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT).*
45. Held, G. (2000*). Server Management: Best Practices*. CRC Press.
46. Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers, *Business History*, 52:6, 978-1002.
47. Hiles, A. (2007). *The Definitive Handbook of Business Continuity Management*. Chichester, England: John Wiley & Sons.
48. Hiles, A. (2014). *Business Continuity Management: Global Best Practices*. Brookfield, SAD: Rothstein Associates.
49. Hockmann, V., Knöll, H. (2008). *Profikurs: Sicherheit von Web-Servern*. Vieweg.
50. Huang, Y., Arsenault, D., Sood, A. (2006). *Closing cluster attack windows through server redundancy and rotations*. Department of Computer Science and Center for Image Analysis. George Mason University, Fairfax.
51. Hubbard, D., W., (2020). *The failure of risk management: why it's broken and how to fix it*. John Wiley & Sons.
52. Hunter, T., Porter, S., Rajan L. (2019). *Building Google Cloud Platform Solutions*, Packt Publishing.
53. Hussain, F. (2017). *Internet of Things: Building Blocks and Business Models*. Springer (2017).
54. Hwang, K., Dongarra, J., Fox, G., C. (2011). *Distributed and Cloud Computing: From Parallel Processing to the Internet of Things*. Morgan Kaufmann.
55. Indira, B. (2016). Cloud Computing: For Business Continuity and Disaster Recovery. *EDU WORLD*, VOL. V, NO. 1.
56. Karim, A. J. (2011). Business Disaster Preparedness: An Empirical Study for measuring the Factors of Business Continuity to fac, e Business Disaster. *International Journal of Business and Social Science*, Vol. 2 No. 18 pp. 183-192.

57. Kassema, J. (2020). Information Technology (IT) Contingency Plan as Part of the Business Continuity Plan: Case of IT Services Delivery Industry. *International Journal of Information Systems & Management Science,* Vol. 12, No. 2,
58. Kernighan, B. (2019). *UNIX: A History and a Memoir*. Kindle Direct Publishing.
59. Kersten, H., Klett, G. (2017). *Business Continuity und IT-Notfallmanagement*, Springer Vieweg Wiesbaden.
60. Khan, U. (2020). Comparative Study of Linux and Windows. *International Journal of Academic Research in Business, Arts and Science, (IJARBAS)*, p. 53-70. Issue: 2, Vol.: 2, Article: 4.
61. Koren, I., Krishna, C. M. (2007). *Fault Tolerant Systems*. San Francisco, SAD: Morgan Kaufmann Publishers.
62. Kranz, M. (2016). *Building the Internet of Things: Implement New Business Models*, Disrupt Competitors, Transform Your Industry. Wiley
63. Kumari, K., A., Sadasivam, G., S., Dharani, D., Niranjanamurthy, M. (2022). *Edge Computing: Fundamentals, Advances and Applications*. CRC Press
64. Kurose, J., F., Ross, K., W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.
65. Kwon, M., Dou, Z., Heinzelman, W., Soyata, T., Ba, H., Shi, J. (2014). Use of network latency profiling and redundancy for cloud server selection. *IEEE International Conference on Cloud Computing.*
66. Lam, W. (2002). *IT Pro: Ensuring Business Continuity*. 1520-9202/02
67. Lee K. (2005). *Building Resilient IP Networks*. Cisco Press.
68. Lewis, S. (2005). Business Continuity and Disaster Recovery Plans – Things Overlooked, *EDPACS*, 33:1, pp. 19-20.
69. Limoncelli, T. A., Hogan, C. J., Chalup, S. R. (2007). *The Practice of System and Network Administration.* Boston, SAD: Pearson.
70. Machida, F., Kawato, M., Maeno, Y. (2010). Redundant virtual machine placement for fault-tolerant consolidated server clusters. *IEEE Network Operations and Management Symposium.*
71. Marcham, A. (2021). *Understanding Infrastructure Edge Computing: Concepts, Technologies, and Considerations*. John Wiley & Sons.
72. McNurlin, B., C., Sprague, R., Bui, T. (2014). *Information Systems Management*. Pearson.
73. Menga, J. (2018). *Docker on Amazon Web Services*. Packt Publishing
74. Menken, I., Blokdijk, G. (2010). *Virtualization: The Complete Cornerstone Guide to Virtualization Best Practices: Concepts, Terms, and Techniques for Successfully Planning, implementing and managing enterprise IT Virtualization Technology*. SAD: Emereo Pty Ltd
75. Mitts, J. (2005). Business Continuity and Disaster Recovery Plans: How and When to Test Them. *EDPACS: The EDP Audit, Control, and Security Newsletter*, 33:5, 8-24

76. Moschovitis, C. (2018). *Cybersecurity Program Development For Business*. New Jersey, SAD: JohnWiley & Sons
77. Mukhopadhyay, S., C. (2014). *Internet of Things: Challenges and Opportunities*. Springer.
78. Nelson, S. (2011). *Pro Data Backup and Recovery*. SAD, Apress.
79. Oggerino, C. (2001). *High Availability Network Fundamentals*. Cisco Press.
80. Peterson, L., L., Davie, B., S. (2022). *Computer Networks: A systems approach*. Morgan Kaufmann.
81. Petković, D., (2020). *Microsoft SQL Server 2019: A Beginner's Guide*. McGraw-Hill Education.
82. Phillips, B., D., Landahl, M. (2020). *Business Continuity Planning: Increasing Workplace Resilience to Disasters*, Elsevier Science.
83. Prakash, S., Mody, S., Wahab, A., Swaminathan, S. (2012). Disaster Recovery Services in the Cloud for SMEs. *International of Cloud Computing, Technologies, Applications & Management* 978-1-4673-4416-6/12.
84. Priyam, P. (2018). *Cloud Security Automation*. Packt Publishing.
85. Rehab, H., Sta, H. (2016). Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs. *Global Summit on Computer & Information Technology* 978-1-5090-2659-3/17.
86. Rezaei, H., Torabi, S. ,Sahebjamnia, N. (2018): Developing a novel quantitative framework for business continuity planning, *International Journal of Production Research.*
87. Rittinghouse, J. W., Ransome, J. R. (2010). *Cloud Computing Implementation,Management and Security*. SAD: CRC Press.
88. Sapapthai, S., Leelawat, N., Tang, J., Kodaka, A., Chintanapakdee, C., Ino, E., i Watanabe, K. (2020). A Stakeholder Analysis Approach for Area Business Continuity Management: A Systematic Review. *J. Disaster Res*., Vol.15, No.5, pp. 588-598.
89. Saquib, Z., Tyagi, V., Bokare, S., Dongawe, S., Dwivedi, M., Dwivedi, J. (2013). A New Approach to Disaster Recovery as a Service over Cloud for Database system. *15th International Conference on Advanced Computing Technologies (ICACT)*
90. Sheeraz, M., Paracha, M., A., Haque1, M., Durad, M., H., Mohsin, S., M., Band, S., S., Amir, M. (2023). Effective Security Monitoring Using Efficient SIEM Architecture. *Human-centric Computing and Information Sciences*, volume 13, Article number: 18
91. Sinclair, B. (2017). *IoT Inc: How your company can use the internet of things to win in the outcome economy*. McGraw-Hill Education.
92. Smith, R., W., (2005). *Linux in a Windows World*. O'Reilly Media.
93. Snedaker, S. (2007). *Business Continuity & Disaster Recovery for IT Professionals*. Burlington, SAD: Syngress Publishing.
94. Speight, P. (2011). Business Continuity, *Journal of Applied Security Research,* 6:4, 529-554.

95. Stamp, M. (2011). *Information Security: Principles And Practice*. New Jearsy, SAD: John Wiley & Sons.
96. Stanton, R. (2005). Beyond disaster recovery: the benefits of business continuity. *Computer Fraud & Security,* Volume 2005, Issue 7, pp.18-19.
97. Šimonova, S. i Šprync, O. (2011). Proactive IT / IS monitoring for business continuity planning. *Ekonomie a Management*, vol 3., s. 57-65.
98. Taheribakhsh, M., Jafari, A., Peiro, M., Kazemifard, N.(2020). 5G Implementation: Major Issues and Challenges. *25th International Computer Conference, Computer Society of Iran (CSICC).*
99. Tanenbaum, A. S. (2003). *Computer Networks*. New Jersey, SAD: Pearson
100. Tanenbaum, A., S., Bos, H. (2014). *Modern Operating Systems*. Pearson
101. Tang, S., Lee, B., He, B. (2014). Towards Economic Fairness for Big Data Processing in Pay-as-you-go Cloud Computing. *IEEE 6th International Conference on Cloud Computing Technology and Science*
102. Turban, E., Volonino, L. (2011). *Information Technology for Management: Improving Strategic and Operational Performance*. John Wiley & Sons.
103. Turban, E., Volonino, L., Wood, G., R. (2013). *Information Technology for Management: Advancing Sustainable, Profitable Business Growth*. John Wiley & Sons.
104. Turner, B. (1978). *Man-made disasters*. London, England: Wykeham.
105. Vasavada. N., Sametriya, D. (2022). *Cracking Containers with Docker and Kubernetes*. BPB Publications.
106. Venkatakrishnan, R. (2014). *Redundancy-based detection of security anomalies in web-server environments.* Faculty of North Carolina State University, Raleigh, North Carolina.
107. W3Techs. (2023). *Usage statistics of web servers*. Pristupljeno: 02.01.2023. Dostupno na: https://w3techs.com/technologies/overview/web_server
108. Wallace, M., Webber, L., (2018). *The Disaster Recovery Handbook*. Amacom.
109. Wang, T., Ma, H., Zhou, Y., Zhang, R., Song, Z. (2015). Fully Accountable Data Sharing for Pay-As-You-Go Cloud Scenes. *Journal Of Latex Class Files,* Vol. 14, No. 8.
110. Whitman, M., E., Mattord, H., J. (2021). *Principles of Incident Response and Disaster Recovery*, Cengage Learning.
111. Winkler, U., Gilani, W., Marshall, A., Guitman, A. (2012). Models and Methodology for Automated Business Continuity Analysis. *IEEE 17th International Conference on Engineering of Complex Computer Systems*, pp. 57-64.
112. Wood, T., Cecchet, E., Ramakrishnan, K., K., Shenoy, P., Merwey, J., Venkataramani, A. (2010). *Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges.* University of Massachusetts Amherst

113. Yang, Y., Chen, X., Tan, R., Xiao, Y. (2021). *Intelligent IoT for the Digital World: Incorporating 5G Communications and Fog/Edge Computing Technologies*. Wiley.
114. Zelenika, R. (2000). *Metodologija i tehnologija izrade znanstvenog i stručnog djela*. Ekonomski fakultet u Rijeci.
115. Zhou, H. (2013). *The internet of things in the cloud: a middleware perspective*. CRC Press.
116. https://ieeexplore.ieee.org/
117. https://www.sciencedirect.com/
118. https://www.researchgate.net/
119. http://scholar.google.com/
120. https://www.semanticscholar.org/