Zaprimljen: 12.6.2025.
Odobren za objavu: 23.7.2025.
Prethodno priopćenje

IZGRADNJA OTPORNOSTI PODUZEĆA S OSVRTOM NA POSLOVNE KRIZE U DIGITALNOM DOBU

Lena Sigurnjak[1], Sanja Knežević Kušljić[1], Ivana Sluganović[2]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: lsigurnjak@unisb.hr
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: sknezevic@unisb.hr
[1] Studentica - Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
ePošta: isluganovic@unisb.hr

Sažetak: Radom se analizira otpornost poduzeća s posebnim naglaskom na poslovne krize u digitalnom dobu. Suočena s nepredvidivim i promjenjivim okruženjem, poduzeća moraju razviti otpornost kako bi se prilagodila tržišnim promjenama i očuvala stabilnost. Teorijski okvir poslovne krize u digitalnom dobu uključuje analizu različitih vrsta poslovnih kriza, jer su krizne situacije jedan od glavnih pokretača neravnoteže na tržištu.
Stoga, svrha rada je da poduzeća moraju adekvatno prilagoditi svoje poslovne strategije kako bi uspješno odgovorili na krizu u kojoj su se našli. Za kvalitetnu prilagodbu kriznim situacijama važno je na vrijeme uočiti problem te razviti poslovne strategije za rješavanje istog. Cilj rada je detaljno obrazložiti opasnosti koje poslovne krize mogu donijeti poduzećima te način na koji digitalizacija poslovanja može utjecati na nastanak krize kao i upravljanje istom. Digitalizacija je sve zastupljenija u poduzećima zbog brojnih prednosti koje donosi poslovanju, stoga je za izgradnju otpornosti poduzeća izuzetno važno uvođenje tehnoloških rješenja i inovacija.
U radu se koriste metode analize, sinteze, indukcije, dedukcije, te deskriptivan metoda za prikaz istraženih pojmova. U istraživačkom djelu rada se provodi istraživanje putem ankete provedeno među 62 ispitanika, a kojim se nastoji istaknuti važnost cyber sigurnost u digitalnom poslovanju te načine na koje se ona može ostvariti.

Ključne riječi: cyber sigurnost, digitalizacija, otpornost, poslovna kriza, tehnologija

1. Uvod

Predmet ovog rada je otpornost poduzeća, odnosno važnost izgradnje otpornosti sustava za uspješno sprječavanje negativnih posljedica poslovne krize. U radu se naglasak stavlja na digitalizaciju sustava koja može pojednostaviti svakodnevne aktivnosti, ali može biti i uzročnik kriznih situacija. Ova tema je izuzetno aktualna za poduzeća jer nastoji istaknuti prednosti digitalizacije sustava te način na koji ona doprinosi izgradnji otpornosti poduzeća. Cilj ovog rada detaljno razložiti i analizirati pojam otpornosti poduzeća, poslovne krize i digitalizacije te prikazati njihov međusobni utjecaj. Za izradu ovog rada bilo je nužno primijeniti niz znanstvenih metoda pomoću kojih se došlo do najrelevantnijih podataka i informacija o navedenom problemu. Najznačajnija metoda je primarno istraživanje kojim se došlo do podataka o strategijama uvođenja digitalizacije poslovanja te načina na koji ona povećava otpornost poduzeća. Budući da krizna situacija, kao i otpornost poduzeća obuhvaća sve dionike unutar poduzeća, metoda dedukcije omogućit će čitatelju sagledavanje šire slike te shvaćanje njihove relevantnosti.

2. Otpornost poduzeća i upravljanje poslovnim rizicima – pregled literature

Poduzeće predstavlja „samostalnu gospodarsku, društvenu i tehničku cjelinu čija je glavna svrha proizvodnja roba i usluga uz racionalnu upotrebu resursa radi ostvarenja dobiti."(Grubišić, 2013., str. 75) Poduzeća organiziraju svoje poslovanje na način da usmjere „prodaju prema maksimalizaciji koristi kako bi ostvarili što veći profit, odnosno kapitalni dobitak" (Benić, 2014., str 7) Može se reći kako su poduzeća generatori poduzetničkih aktivnosti kroz koje poduzetnik razvija svoje ideje i stvara inovacije. Za poduzetnike se stoga može zaključiti kako su oni osobe koje pokreću inovacije i korištenje „tehnologije u poslovanju kako bi unaprijedili postojeću tehnološku strukturu" (Buble, 2006., str. 5) svog poduzeća.

Zbog očuvanja stabilnosti sustava poduzeća najprije moraju „utvrditi vjerojatnost krize, a zatim razmotriti posljedice iste za organizaciju ili mogući učinak na poslovanje." (Tafra-Valović, 2011., str 73) Na taj način poduzeća mogu stvoriti razinu otpornosti koja će im omogućiti neometano poslovanje bez gubitaka.

Organizacijska otpornost važna je kako bi poduzeća osigurala prilagodljivost i sposobnost oporavka dok prolaze kroz poslovne krize, poremećaje ili promjene.(Premiere continuum) Može se zaključiti kako je otpornost poduzeća strateški imperativ za organizacije jer omogućuje poduzećima dugoročno poslovanje i napredovanje, posebice u usporedbi s organizacijama koje ne ulažu u otpornost.

Poduzeća koja ulažu u otpornost poslovanja usmjerena su na „zaštitu i svijest od rizika, konkurentsku prednost, strateško upravljanje te otpornost u opskrbnim lancima." (Reinmoeller, 2005.) Zaštita i svijest o rizicima omogućuju poduzećima pravovremeno prepoznavanje prijetnji te ublažavanje tržišnih rizika putem različitih „internih i eksternih strategija." (Duchek, 2016.)

Organizacijska otpornost se tako sastoji od „faze aktivacije, odgovora i organizacijskog učenja." (Duchek , Raetze, 2019.) Ove faze zapravo predstavljaju životni vijek trajanja otpornosti. „Otpornost ne nastaje nužno kao rezultat krize, ona se može svjesno razvijati" (Karabatić, Skendrović, 2020.) kroz odgovarajuće organizacijske strategije čime postaje ključan resurs za dugoročni uspjeh. Stoga se organizacijska otpornost ne treba shvaćati isključivo kao reakcija na izvanredne okolnosti već kao strateška sposobnost koju treba graditi prije same krizne situacije. Otpornost osigurava poduzećima stabilnost, održava konkurentnost te prilagodljivost dinamičnom poslovnom okruženju.

Organizacijsko učenje jedna je od najvažnijih faza u razvoju otpornosti jer se uočava „djelovanje organizacije u kriznoj situaciji na svim razinama."(Jugo, 2017., str 231) Poduzeća nakon krize trebaju iznova analizirati aktivnosti koje su poduzete u fazi aktivacije i tijekom krize u fazi odgovora, na taj način organizacije se mogu brže prilagoditi i učvrstiti svoju otpornost.

Organizacijska otpornost ne samo da pomaže poduzećima u izlasku iz krize nego „potiče stratešku prilagodbu i korištenje takvih izazova za rast i razvoj organizacijske strukture." (Mancini, 2021.) Organizacije koje prihvaćaju otpornost mogu napredovati, tako što pretvaraju potencijalne slabosti u prilike što osigurava povećanje konkurentske prednosti i dugoročni napredak.

3. Utjecaj digitalizacije na nastanak i upravljanje poslovnom krizom

U digitalnom dobu, otpornost poduzeća poprilično ovisi o njihovoj sposobnosti primjene tehnoloških rješenja koja omogućuju bržu prilagodbu tržišnim promjenama, unapređenje poslovnih procesa i osiguravanje kontinuiteta poslovanja. Osim povećanja brzine u komuniciranju i obavljanju svakodnevnih poslovnih aktivnosti, digitalizacija također povećava sigurnost podataka i

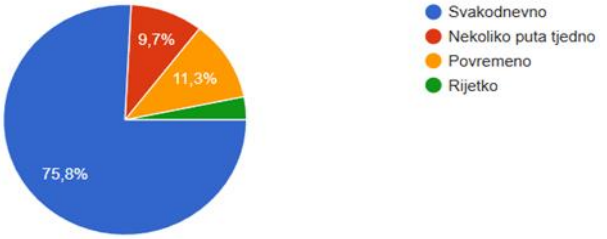
smanjenje operativnih troškova. (Raunaq, 2024.) Sigurnost poslovanja jedan je od temeljnih elemenata otpornosti poduzeća jer se na taj način osigurava zaštita osjetljivih informacija i smanjenje rizika od vanjskih prijetnji posebice kibernetičkih napada. Glavne vrste kibernetičkih napada odnose se na „prijetnje ucjenjivačkim softverom, povrede podataka i probleme sa cloud tehnologijom." (Sprčić, Lacković, str 174) Svaki od navedenih napada može ozbiljno naštetiti povjerljivim podatcima poduzeća te ograničiti njihovu otpornost. Kako bi poduzeća osigurala kvalitetnu implementaciju tehnoloških rješenja potrebno je poduzeti „ključne korake za tehnološku otpornost." (Pozhueva, 2024.) Prvi korak jest prepoznavanje najkritičnijih poslovnih procesa na osnovu kojih se prikuplja i analizira podatke kako bi se procijenila otpornost promatranih elemenata i odredili prioriteti za poboljšanje.

4. Metodologija istraživanja

U ovom poglavlju bit će navedeni i prikazani podatci koji su prikupljeni na temelju anketnog upitnika koji je proveden online. Rezultati istraživanja prikupljeni su putem 62 uzoraka, pri čemu uzorak predstavlja dio osnovnog statističkog skupa koji služi za dobivanje rezultata koji se kasnije može analizirati i prikazati. Anketa je bila sastavljena od slijeda logičnih pitanja pri čemu je korištena Likertova skala putem koje ispitanici mogu izraziti negativan ili pozitivan stav prema nekom od ponuđenih odgovora. Kroz odgovore ispitanika vidljivo je njihovo slaganje, to jest ne slaganjem s određenim pitanjem ili tvrdnjom. Kako bi se ispitanicima pružila mogućnost detaljnijih odgovora, korištena je i Thurstonova skala pomoću koje su se dobili precizniji odgovori i mišljenja ispitanika.

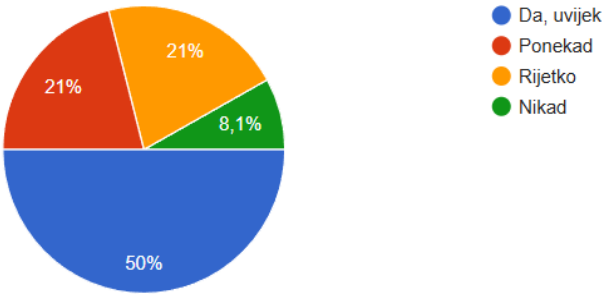
5. Rezultati istraživanja

U istraživanju su sudjelovala 62 ispitanika, od kojih je 21% muškog spola, a 79% ženskog spola. Dobna skupina ispitanika: 48% je u dobi 18-25 godina, ispitanici od 35-45 35-45, te 55 i više godina su najmanje zastupljeni samo 8,1% po razredu, a ispitanici u dobi od 25-35 godina su zastupljeni u postotku od 29%. 58% ispitanika su zaposleni, 35,5% je studentska populacija, a ostali spadaju u populaciju učenika, umirovljenika i nezaposlenih. U nastavku slijedi grafički prikaz podataka.



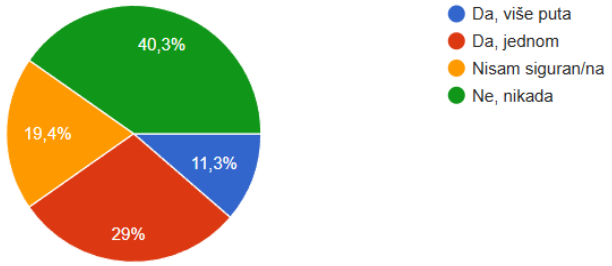
Grafikon 1. razina korištenja internetskih usluga

Grafikon 1. prikazuje razinu korištenja Interneta i internetskih usluga od strane ispitanika. Vidljivo je kako čak 75,8% ispitanika svakodnevno koristi Internet za različite potrebe, dok 11,3% njih Internet koriste povremeno. Najmanji broj ispitanika od svega 3,2% rijetko koriste Internet, a 9,7% koriste usluge nekoliko puta tjedno.



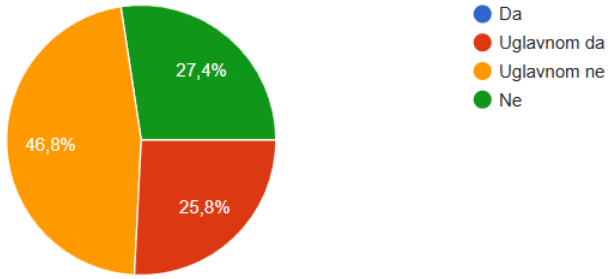
Grafikon 2. Zaštita podataka

Grafikon 2 ukazuje na to kako je broj ispitanika koji su oprezni prilikom korištenja interneta čak 50%, dok njih 42% rijetko ili ponekad štite svoje podatke putem antivirusnih ili drugih softvera. 8,1% ispitanika nikad ne koriste zaštitne softvere na svojim podatcima, stoga postoji povećana opasnost od krađe i zlouporabe osobnih podataka.



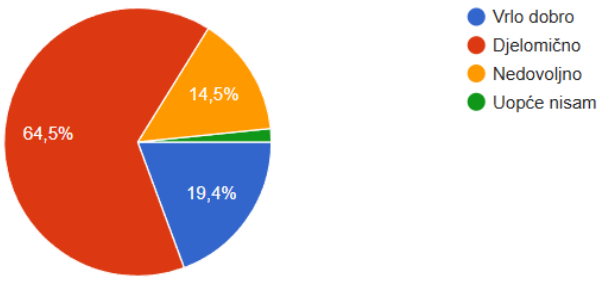
Grafikon 3. Zlouporaba osobnih podataka

Podatci iz grafikona 3. ukazuju na to kako je čak 40 % ispitanika doživjelo krađu ili zlouporabu podataka barem jednom (29%) ili više puta (11,3%). Takvi rezultati upućuju na rastući broj hakera i kradljivaca koji koriste Internet kako bi došli do povjerljivih podataka. Međutim 40% ispitanika nikad se nije susrelo s krađom podataka, bilo radi dobre zaštite ili opreza prilikom dijeljenja istih, dok 19,4% ispitanika nije sigurno jesu li ikad doživjeli zlouporabu osobnih podataka.



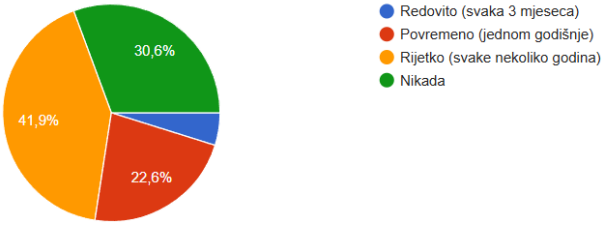
Grafikon 4. Razina sigurnosti podataka na društvenim mrežama

Najveći broj ispitanika, odnosno njih 46,8% slaže se kako online platforme uglavnom ne pružaju dovoljnu sigurnost za osobne podatke, dok 25,8% njih smatra kako su podatci uglavnom sigurni. Prema tome se može zaključiti kako su ispitanici upoznati s rastućim brojem online prijevara te kako se ne osjećaju sigurno prilikom korištenja online platformi i društvenih mreža.



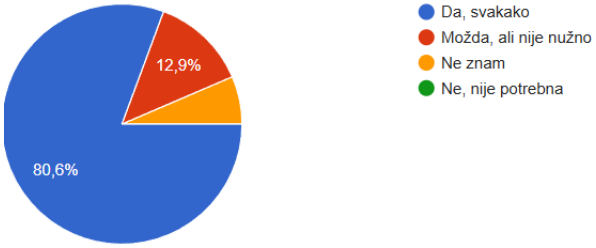
Grafikon 5. Privatnost i zaštita podataka na internetu

Prema podatcima prikazanim na grafikonu 5. može se iščitati kako je većina ispitanika samo djelomično upoznata s zaštitom podataka na internetu (64,5%), dok je njih 19,4% vrlo dobro informirano o navedenoj tematici. 14,5% ispitanika prepoznaje kako su nedovoljno upoznati sa privatnošću i zaštitom podataka, a 1,6% ispitanika uopće nisu upoznati s navedenim. Rezultati ukazuju na to kako su ispitanici u većini samo djelomično svjesni značenja privatnosti i zaštite osobnih podataka te da na tome trebaju poraditi kako bi izbjegli moguće opasnosti.



Grafikon 6. Sigurnosne lozinke

Većina ispitanika svoje sigurnosne lozinke ne mijenjaju nikada (30,6%) ili rijetko (41,9%), odnosno svakih nekoliko godina. 22,6% ispitanika svoje lozinke mijenja na godišnjoj razini, dok samo 4,8% njih mijenja lozinke svaka 3 mjeseca. Ovi rezultati mogu ukazati na to kako su ispitanici previše sigurni u jačinu svojih lozinki te postoji pretpostavka da koriste iste lozinke za više različitih uređaja ili platformi.



Grafikon 7. Edukacija o cyber sigurnosti

Posljednji grafikon odnosi se na edukaciji o cyber sigurnosti, pri čemu je dio ispitanika izrazio kako je edukacija

svakako potrebna (80%), dok su drugi ispitanici neodlučni (6,5%) ili smatraju kako je edukacija poželjna, ali nije nužna (12,9%). Prema rezultatima vidljivo je kako većina ispitanika stavlja edukaciju na prvo mjesto kad je riječ o korištenju interneta i dijeljenju podataka.

6. Rasprava

Na osnovu svega izrečenog prilikom provedenog istraživanja može se zaključiti kako je cyber sigurnost relevantno nov pojam stoga većina ljudi nije u potpunosti upoznata s njegovim značenjem. Međutim s obzirom na to da skoro svi ispitanici svakodnevno koriste internet u različite svrhe, potrebno je povećati svijest o važnosti ove tematike. Može se zaključiti kako je cyber sigurnost zastupljen pojam, ali ima prostora za napredak.

7. Zaključak

Na osnovu rezultata istraživanja može se zaključiti kako je cyber sigurnost relevantno nov pojam stoga većina ljudi nije u potpunosti upoznata s njegovim značenjem. Međutim s obzirom na to da skoro svi ispitanici svakodnevno koriste internet u različite svrhe, potrebno je povećati svijest o važnosti ove tematike. Ono što je važno napomenuti jesu iskustva s krađama identiteta jer je istraživanje pokazalo da je čak 40% ispitanika doživjelo takve situacije jednom ili više puta. Zbog toga je važno educirati se o zaštiti podataka te koristiti različite mjere sigurnosti poput antivirusnih softvera koji će pravovremeno ukazati na potencijalnu opasnost.

8. Literatura

Benić, Đ. (2014). Uvod u ekonomiju, Zagreb, Školska knjiga

Buble, M. (2006). Poduzetništvo: realnost sadašnjost i izazov budućnosti, Split, RRiF-plus d.o.o.

Duchek S., Raetze S.: The Role of Diversity in Organizational Resilience: A Theoretical Framework, (2019.) preuzeto s: https://link.springer.com/article/10.1007/s40685-019-0085-7 Pristupljeno (05.04.2025.)

Duchek S.: Organizational resilience: a capability-based conceptualization, (2019.) preuzeto s: https://link.springer.com/article/10.1007/s40685-019-0085-7 Pristupljeno (05.04.2025.)

Grubišić, D. (2013). *Poslovna ekonomija*, Split, Ekonomski fakultet Sveučilišta u Splitu

Jugo, D. (2017). *Menadžment kriznog komuniciranja*, Zagreb, Školska knjiga

Karabatić, M., Skendrović, K.: Kompetencije zaposlenika kao ključan čimbenik otpornosti poslovanja, (2020.) Preuzeto s: https://dku.hr/wp-content/uploads/2020/10/DKU2020_zbornik-v2.pdf Pristupljeno (08.04.2025.)

Mrnjavac, Ž., Kordić, L., Šimunović, B. (2019). *Osnove ekonomije 2*, Zagreb, ALKA

Osmanagi Bedenik, N.: CRISIS MANAGEMENT: THEORY AND PRACTICE, (2010.) preuzeto s: https://hrcak.srce.hr/file/87513 Pristupljeno (10.04.2025.)

Pozhueva, T.: Digital Innovation for Crisis Management, (2024.). preuzeto s: https://www.researchgate.net/publication/384004881_Digital_technologies_in_crisis_managemen t Pristupljeno (10.05.2025.)

Premiere continuum: What is organizational resilience and why is it important? Preuzeto s: https://www.premiercontinuum.com/resources/organizational-resilience-definition Pristupljeno (02.04.2025.)

Raunaq R.,: Role of Technology in Building Resilient Companies of the Future, (2024.) preuzeto s: https://www.aranca.com/knowledge-library/articles/business-research/role-of-technology-in-building-resilient-companies-of-the-future?utm Pristupljeno (17.04.2025.)

Reinmoeller P.: The Link Between Diversity and Resilience, (2005.), preuzeto s https://www.researchgate.net/publication/40968887_The_Link_Between_Diversity_and_Resilience Pristupljeno (04.04.2025.)

Sprčić Miloš, D, Lacković I.: U*pravljanje rizicima: teorijski koncepti i primjena u poslovnoj praksi,* Zagreb. Naklada SLAP
Tafra-Vlaović, M. (2011). *Upravljanje krizom,* Zaprešić

BUILDING CORPORATE RESILIENCE WITH A FOCUS ON BUSINESS CRISES IN THE DIGITAL AGE

Abstract: The paper analyzes corporate resilience with a special emphasis on business crises in the digital age. Faced with an unpredictable and changing environment, companies must develop resilience in order to adapt to market changes and maintain stability. The theoretical framework of business crises in the digital age includes the analysis of different types of business crises, because crisis situations are one of the main drivers of market imbalance.
Therefore, the purpose of the paper is that companies must adequately adjust their business strategies in order to successfully respond to the crisis they find themselves in. For quality adaptation to crisis situations, it is important to identify the problem in time and develop business strategies to solve it. The aim of the paper is to explain in detail the dangers that business crises can bring to companies and the way in which the digitalization of business can affect the emergence of a crisis as well as its management. Digitization is increasingly common in companies due to the numerous advantages it brings to business, therefore, the introduction of technological solutions and innovations is extremely important for building the resilience of companies.
The paper uses methods of analysis, synthesis, induction, deduction, and a descriptive method to present the researched concepts. In the research part of the work, a survey is conducted among 62 respondents, which aims to highlight the importance of cyber security in digital business and the ways in which it can be achieved.

Keywords: business crisis, cyber security digitization, resilience, technology