DIGITALIZACIJA – NAČRTOVANJE

BORUT JEREB
Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
borut.jereb@um.si

Elektronsko poslovanje (e-poslovanje) igra ključno vlogo v sodobnem digitalnem okolju, preoblikuje poslovne prakse in odpira nove možnosti. Predstavljen je model vrednostne verige e-poslovanja, ki zajema podporne procese, vrednostno verigo in tehnološke rešitve. Poleg tega so obravnavani različni pristopi e-poslovanja, vključno z e-marketingom, e-dokumentacijo, e-plačili in e-upravljanjem s strankami. V nadaljevanju je poudarjena pomembnost informacijske in kibernetske varnosti v sodobnem poslovnem okolju. Varovanje digitalne pokrajine postaja ključno, pri čemer informacijska varnost zajema zaščito informacij, medtem ko kibernetska varnost obravnava zaščito digitalnih sistemov pred kibernetskimi grožnjami. Obe disciplini sta ključni za ohranjanje zaupanja in varnosti pri e-poslovanju. Na koncu prispevka je predstavljeno upravljanje IT tveganj s pomočjo standarda ISO/IEC 27005.

DOI
https://doi.org/10.18690/um.fl.2.2025.1

ISBN
978-961-286-971-7

Ključne besede:
digitalizacija,
e-poslovanje,
informacijska varnost,
kibernetska varnost,
IT tveganja

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fl.2.2025.1

ISBN
978-961-286-971-7

Keywords:
digitalization,
e-business,
information security,
cyber security,
IT risks

DIGITALIZATION – PLANNING

BORUT JEREB
University of Maribor, Faculty of Logistics, Celje, Slovenia
borut.jereb@um.si

E-business plays a crucial role in the modern digital environment, transforming business practices and opening new possibilities. The model of the e-business value chain is presented, encompassing supporting processes, the value chain, and technological solutions. Additionally, various e-business approaches are addressed, including e-marketing, e-documentation, e-payments, and e-customer management. The importance of information and cyber security in the contemporary business environment is emphasized. Safeguarding the digital landscape becomes crucial, with information security covering the protection of information, while cyber security addresses the protection of digital systems from cyber threats. Both disciplines are essential for maintaining trust and security in e-business. The article concludes with the presentation of IT risk management using the ISO/IEC 27005 standard.

University of Maribor Press

1 Uvod

V hitro spreminjajočem se okolju digitalne dobe se je elektronsko poslovanje ali e-poslovanje pojavilo kot usmeritev in pot, ki spreminja način, kako organizacije izvajajo svoje operacije in komunicirajo z deležniki. Pri podjetjih se e-poslovanje nanaša na uporabo digitalnih tehnologij in interneta za poenostavitev in izboljšanje različnih poslovnih procesov; od nakupovanja in prodaje blaga ter storitev do upravljanja notranjih operacij in sodelovanja s partnerji. Pri trgovanju pa, za razliko od tradicionalnih poslovnih modelov, e-poslovanje presega geografske omejitve in časovno omejenost, tako da zagotavlja globalno platformo za trgovino.

Obsega širok spekter spletnih dejavnosti, vključno z e-trgovino, e-marketingom, e-upravljanjem dobavnih verig in e-nabavo. Integracija tehnologije ne le omogoča bolj učinkovite in stroškovno smotrne poslovne prakse, temveč odpira tudi nove možnosti za inovacije in prilagajanje trgu.

Ključni elementi e-poslovanja vključujejo vzpostavitev prisotnosti na spletu, izvajanje varnih elektronskih transakcij, izkoriščanje podatkovne analitike za informirano odločanje ter prilagajanje nenehno spreminjajočemu se digitalnemu okolju. Uspeh podjetja v okolju e-poslovanja je odvisen od njegove sposobnosti ustvarjanja brezhibnih in privlačnih izkušenj za stranke, vzpostavljanja zaupanja in varnosti pri spletnih transakcijah ter izkoriščanja vpogledov, pridobljenih iz (največkrat masivnih) podatkov, da ostane podjetje konkurenčno na dinamično spreminjajočem se trgu.

Ker tehnologija nenehno napreduje in se spreminja, bo e-poslovanje igralo vse pomembnejšo vlogo pri oblikovanju prihodnosti poslovanja v podjetju in med podjetji – predvsem, ko govorimo o oskrbovalnih verigah. Ne glede na to, ali gre za zagonsko podjetje ali uveljavljeno multinacionalko, je razumevanje in izkoriščanje moči e-poslovanja ključno za uspeh pri poslovanju v okolju digitalne ekonomije. Pri tem podjetja ne smejo premagovati le tehnoloških izzivov, temveč tudi spreminjajoča se pričakovanja pri povezovanju z digitalno veščimi zaposlenimi in kupci znotraj in zunaj meja samega podjetja.

V nadaljevanju želimo bralca napotiti v iskanje poti za to, da bo znal:

- pregledati in analizirati tisti del poslovanja v njegovem okolju, ki bi ga bilo smiselno digitalizirati,
- prepoznati pomen informacijske in kibernetske varnosti in ju kot taki znati načrtovati v vlogi srednjega upravljavskega sloja
- ter kritično ovrednotiti IT tveganja v vlogi srednjega upravljavskega sloja.

2 e-poslovanje

E-poslovanje je celovit pristop k izvajanju poslovnih procesov s pomočjo elektronskih sredstev. To velja tudi za izvajanje poslovnih procesov, ki podpirajo izvajanje logističnih procesov. Obsega širok nabor dejavnosti, ki izkoriščajo digitalne tehnologije za optimizacijo operacij, izboljšanje izkušenj strank in povečanje splošne učinkovitosti poslovanja. E-poslovanje vključuje tako notranje kot zunanje interakcije organizacij in si prizadeva preoblikovati tradicionalne poslovne prakse s povezovanjem elektronskih sistemov in komunikacijskih kanalov. Koncept e-poslovanja spreminja način, kako organizacije izvajajo svoje operacije, komunicirajo s strankami in ustvarjajo vrednost. Predstavlja celovit premik k izvajanju poslovnih procesov z elektronskimi sredstvi, spodbuja učinkovitost, inovacije in globalni doseg.

Izvor e-poslovanja sega v zgodnje dni interneta. Z nastankom e-poslovanja (e-trgovine) je bila vpeljana zamisel o nakupovanju in prodaji izdelkov na spletu. Vendar se je s časom razvijala tudi zamisel o e-poslovanju, ki obsega množico dejavnosti, ki se raztezajo daleč preko digitalnih trgovin.

E-poslovanje je tako sestavljeno iz poslovanja, ki bazira na informacijsko-komunikacijskih tehnologijah (IKT). Nekatera ključna področja takšnega poslovanja so:

- **e-marketing**: uporaba digitalnih kanalov, kot so: socialna omrežja, e-poštni marketing, optimizacija spletnih iskalnikov (SEO) in spletno oglaševanje za promocijo izdelkov ali storitev ter dosego širšega občinstva.

- **E-trgovina:** kot že omenjeno, je e-trgovina pomemben del e-poslovanja. Vključuje spletno kupovanje in prodajo blaga ter storitev, zajema različne poslovne modele in platforme.
- **E-upravljanje s strankami (e-CRM)**: upravljanje in negovanje odnosov s strankami s pomočjo digitalnih orodij in platform. To vključuje sledenje interakcijam s strankami, analizo podatkov za prilagajanje izkušenj ter zagotavljanje učinkovite podpore strankam preko spleta.
- **E-upravljanje oskrbovalne verige (e-SCM)**: uporaba digitalnih tehnologij za optimizacijo procesov v oskrbovalni verigi; od nabave in upravljanja zalog do izpolnjevanja naročil in distribucije.
- **E-nabava**: uporaba elektronskih sistemov za upravljanje nabave blaga in storitev, vključno z izbiro dobaviteljev, izdajanjem naročil in upravljanjem odnosov z dobavitelji.
- **E-sodelovanje**: omogočanje sodelovanja med zaposlenimi in partnerji preko digitalnih platform, videokonferenc in orodij v oblaku.
- **E-upravljanje z znanjem**: upravljanje in deljenje organizacijskega znanja elektronsko za izboljšanje odločanja, reševanja problemov in inovacij.
- **E-analiza podatkov in poslovna inteligenca**: uporaba orodij za analizo podatkov za pridobivanje vpogleda iz obsežnih naborov podatkov, kar omogoča odločanje na podlagi podatkov.
- **E-plačila in finančne transakcije**: obdelava elektronskih plačil, spletno izdajanje računov in varno upravljanje finančnih transakcij preko digitalnih platform.

V nadaljevanju so naštete nekatere koristi, ki so pogojene z značilnostmi e-poslovanja. Ključne sestavine in vplivi e-poslovanja so:

- **digitalna transformacija**: e-poslovanje je pospešilo proces digitalne transformacije v vseh panogah. Organizacije so prešle iz tradicionalnih poslovanj v integrirane digitalne ekosisteme, ki poenostavljajo procese, izboljšujejo izkušnje strank in povečujejo celotno učinkovitost.
- **Globalni doseg**: e-poslovanje omogoča podjetjem, da dosežejo globalno občinstvo brez omejitev geografskih meja.
- **Učinkovito nižanje stroškov**: digitalni procesi lahko znižajo operativne stroške, kot so dokumentacija na papirju in fizična infrastruktura. Priča smo

novim ekonomskim modelom in priložnostim za zaposlovanje. Začetniki in podjetniki lahko nastopajo in se vključujejo v globalne trge z minimalnimi vstopnimi ovirami, kar spodbuja gospodarsko rast.

- **Poudarek na strankah/partnerjih**: e-poslovanje omogoča prilagojene interakcije, hitre odzive in priročen dostop do informacij, kar povečuje zadovoljstvo strank. Stranke in/ali partnerji so v središču (poslovnih) operacij. S pomočjo podatkov, ki temeljijo na analitiki, organizacije razumejo želje, vedenje in potrebe strank in partnerjev, kar vodi v prilagojene interakcije in ponudbe.
- **Optimizirani procesi**: avtomatizacija nalog in procesov vodi v večjo učinkovitost in zmanjšanje števila človeških napak. Avtomatizacija, integracija in digitalizacija procesov povečujejo operativno učinkovitost. Od upravljanja dobavne verige do nadzora zalog in obdelave naročil, e-poslovanje optimizira uporabo virov in znižuje stroške.
- **Vpogledi v masovne podatke in odločanje na podlagi podatkov**: e-poslovanje ustvarja dragocene podatke, ki jih je mogoče analizirati, da bi dobili vpogled v obnašanje strank, trende na trgu in poslovno uspešnost.
- **Konkurenčna prednost**: organizacije, ki sprejemajo strategije e-poslovanja, so bolje pozicionirane za prilagajanje spreminjajočim se tržnim razmeram in preseganje konkurence.
- **Inovacije in agilnost**: e-poslovanje spodbuja okolje inovacij. Organizacije se hitro prilagajajo spreminjajočim se dinamikam trga, uvajajo nove storitve in izdelke ter preizkušajo nove poslovne modele brez zamud. Hitro in skoraj v realnem času.

Tako e-poslovanje zajema različne vidike sodobnih poslovnih operacij, ki izkoriščajo digitalne tehnologije za izboljšanje učinkovitosti, vključevanje strank ter splošno konkurenčnost. Gre za sprejemanje celostnega pristopa k upravljanju poslovanja v digitalni dobi.

E-poslovanje tako ponuja številne prednosti, kot so večji doseg, prihranek stroškov in udobje, ima pa tudi več negativnih vidikov, ki jih morajo podjetja upoštevati in obravnavati, da zagotovijo trajnostno in uspešno spletno poslovanje. To vključuje vlaganje v robustne varnostne ukrepe, učinkovito upravljanje logistike, zagotavljanje

skladnosti s pravnimi predpisi ter vzpostavljanje zaupanja in zadovoljstva strank z zanesljivimi storitvami in varnimi transakcijami.

Nekateri ključni negativni vidiki e-poslovanja, ki jih je potrebno še posebej pozorno nasloviti pri e-poslovanju, so:

- **varnostni izzivi:** e-poslovanje vključuje prenos občutljivih podatkov, vključno s finančnimi transakcijami in osebnimi informacijami. To pomeni, da je e-poslovanje tarča kibernetskih napadov, kot so hekerski vdori, "phishing" in zlonamerna programska oprema. Podjetja morajo veliko vlagati v kibernetsko varnost, da zaščitijo podatke, kar je lahko drago in zapleteno.
- **Izziv zasebnosti:** z zbiranjem ogromnih količin podatkov o potrošnikih se pojavijo resni pomisleki glede zasebnosti. Podjetja morajo zagotoviti, da upoštevajo predpise o varstvu podatkov, kot je GDPR. Neupoštevanje teh predpisov lahko povzroči pravne posledice in izgubo zaupanja strank.
- **Tehnične težave:** e-poslovanje močno temelji na tehnologiji. Tehnične težave, kot so izpadi spletnih strani, programske napake ali počasno nalaganje, lahko motijo poslovanje, kar vodi do izgube prodaje in nezadovoljnih strank.
- **Visoki začetni stroški:** vzpostavitev robustne infrastrukture za e-poslovanje je lahko drago. To vključuje stroške razvoja uporabniku prijazne spletne strani, obratovanje varnih plačilnih sistemov in integracijo potrebnih zalednih sistemov. Ti začetni vložki so lahko ovira za mala podjetja.
- **Intenzivna konkurenca:** internet je v mnogih segmentih delovanja izenačil pogoje za delovanje največjih in najmanjših podjetij. Povečana konkurenca otežuje, da bi podjetja izstopala in privabljala stranke, kar pogosto zahteva znatne naložbe v trženje in strategije diferenciacije.
- **Logistični izzivi:** e-poslovna podjetja morajo še dodatno pozornost posvetiti upravljanju logističnih procesov. To vključuje skladiščenje, upravljanje zalog, pošiljanje in obdelavo vračil. Slabo upravljanje logistike lahko povzroči zamude pri dostavi in povišane stroške, kar negativno vpliva na zadovoljstvo strank.
- **Odvisnost od tehnologije:** pri e-poslovanju so podjetja zelo odvisna od tehnologije, kar pomeni, da lahko katerakoli tehnološka okvara ustavi

poslovanje. Podjetja morajo imeti robustno IT podporo in načrte za obnovitev po nesrečah, da bi zmanjšala IT tveganja.

- **Zaupanje in zadovoljstvo strank:** vzpostavljanje zaupanja s strankami je na spletu bolj zahtevno kot v fizičnih trgovinah. Težave, kot so nezmožnost fizičnega pregleda izdelkov pred nakupom, skrbi glede varnosti plačil in zamude pri odzivanju na poizvedbe strank, lahko zmanjšajo zadovoljstvo strank.
- **Pravna in regulativna skladnost:** pri e-poslovanju se morajo podjetja spoprijeti z zapleteno mrežo predpisov, ki se razlikujejo glede na regijo in industrijo. Ti vključujejo zakone o varstvu potrošnikov, predpise o elektronskem poslovanju in mednarodne trgovinske zakone. Neskladnost lahko privede do glob in drugih težav pri doseganju pravnih norm.
- **Pomanjkanje osebne interakcije:** pomanjkanje osebne interakcije v e-poslovanju otežuje vzpostavljanje poglobljenih odnosov s strankami. Osebnostno naravnane storitve in človeški stiki pogosto igrajo ključno vlogo pri zvestobi in zadovoljstvu strank.
- **Upravljanje vračil in povračil:** upravljanje vračil in povračil v e-poslovanju je lahko bolj zapleteno in drago kot v tradicionalni trgovini. Postopek vključuje obdelavo obratne logistike, ponovno založitev in obravnavanje morebitne izgube ali poškodbe vrnjenih predmetov.
- **Digitalni razkorak:** niso vsi potencialni kupci enako dostopni do interneta ali digitalnih naprav, kar vodi do digitalnega razkoraka. To omejuje doseg e-poslovanja podjetij, zlasti v regijah z nizko internetno penetracijo ali med demografskimi skupinami z manj tehnološke pismenosti.

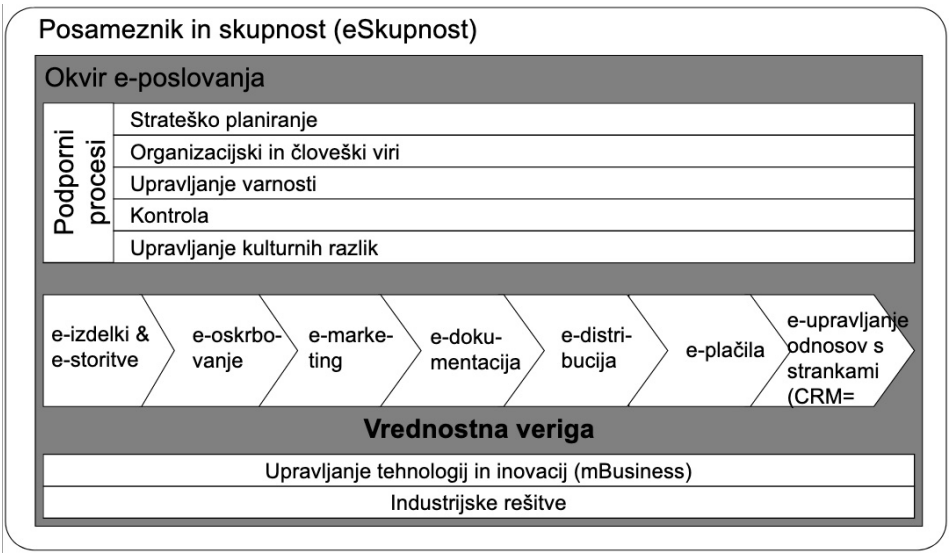
2.1 Model e-poslovanja

Na sliki 1.1 je prikazan model vrednostne verige e-poslovanja po knjigi Meier & Stormer (Meier, 2009). Slika prikazuje tri bistvene sestavine e-poslovanja, ki so:

- podporni procesi za izvajanje e-poslovanja,
- vrednostna veriga e-poslovanja,
- tehnično-tehnološke rešitve za podporo izvajanja e-poslovanja.

Podporne procese sestavljajo: strateško načrtovanje, organizacijski in kadrovski viri, upravljanje informacijske in kibernetske varnosti, kontrola ter upravljanje kulturnih razlik. Vsi ti procesi so pogojeni in so v zvezi z e-poslovanjem. Predpostavljamo, da je znanje o teh procesih že prisotno ali pa ga je treba pridobiti iz literature o managementu.

Vrednostno verigo sestavlja sedem različnih pristopov, ki pa se medsebojno dopolnjujejo in v vsakem od omenjenih pristopov je mogoče najti druge pristope. Pa vendar, na levi strani te vrednostne verige so pristopi, ki zahtevajo nižje vložke, praviloma tudi dajejo rezultate nižje vrednosti. Bolj, kot gremo proti desni, večji so vložki za realizacijo rešitve in pričakovane so večje koristi.



Slika 1.1: Model e-poslovanja
Vir: A. Meier & H. Stormer

Pri organizaciji elektronskih izdelkov in storitev je naloga organizacije najti ustrezno obliko sodelovanja s pomočjo poslovnega modela. Takšne oblike sodelovanja med organizacijami in morebitnimi kupci segajo od povsem enostavne in informativne predstavitve blaga, odprtih tržnic z blagom in njenimi vrednostmi, pa do bolj zaprtih sistemov, kjer deležniki takšne tržnice medsebojno sodelujejo.

Naslednji pristop pri e-poslovanju je namenjen elektronsko podprtim nabavnim postopkom. Načeloma obstaja vrsta rešitev za e-oskrbovanje. Rešitve se medsebojno razlikujejo glede na to, ali so katalogi izdelkov in storitev za izbiro in nabavo izdelkov na voljo na strani kupca (buy side) ali na strani dobavitelja (sell side). V tretji varianti (elektronski trg) tretja stranka zagotavlja programske rešitve in kataloge za nabavo. Tako se lahko uporabljajo primerjave in vrednotenje izdelkov in storitev. Upravljanje katalogov predstavlja poseben izziv.

e-marketing (ali spletni marketing) deluje tako, da s pomočjo elektronskih sredstev pridobivanja informacij in komuniciranja izkorišča tržne potenciale in neguje poslovne odnose. Segmentacija spletnih »kupcev« na kategorije omogoča izvajanje raznolikega marketinškega procesa in takojšnjega prilagajanja storitev spletnega marketinga. Prvi uspešni globalni primer tovrstnega e-poslovanja je bilo podjetje Google. Sledil je Facebook in ostali. Z ustreznimi ključnimi kazalci omogočajo merjenje učinkovitosti ponudb preko spleta (na primer z uporabo spletnega brskalnika), izračunavajo lahko stopnje interakcije (če govorimo, da je na drugi strani spletni potrošnik), spodbujajo spletne stranke k ustvarjanju njihovih (lahko navideznih) vrednosti, izvedejo poslovne transakcije (spletni kupec) ter vzdržujejo povezave s stranko (spletni ključni kupec). Pri tem je seveda treba preučiti in analizirati posebnosti spletnega oglaševanja.

Naslednji pristop se ukvarja s konceptom e-dokumentacije. Tu se elektronski dokument obravnava kot pravno veljaven dokument. Da bi to dosegli, je treba vzpostaviti zaupanja vredne centre, ki registrirajo dejanske osebe, izdajajo digitalna potrdila in zagotavljajo par elektronskih ključev za digitalni podpis. Asimetrični kriptografski postopki, ki uporabljajo zasebne in javne ključe, so osnovna zahteva pri uporabi takšnih potrdil in podpisov. Elektronski dokumenti se lahko elektronsko podpišejo na eni strani, na drugi strani pa se lahko izvede avtentikacija digitalnega podpisa. Dokumente lahko tudi ustrezno pretvorimo v elektronski kriptogram, ki dokaj dobro zaščiti dokument pred nezaželenimi vpogledi.

Pri elektronsko podprti distribuciji izdelka ali storitve, ki lahko nastopata v fizični ali elektronski obliki, govorimo o naslednji stopnji kompleksnosti elektronskega poslovanja. Če ima potrošnik za storitev pri roki mobilno napravo z internetno povezavo, lahko izkoristi časovno in lokacijsko neodvisen nakup ali storitev (spletna distribucija). Seveda, se tudi izdelki v elektronski obliki lahko distribuirajo na klasičen

način – to je ne po elektronski poti, saj ima tudi distribucija brez povezave v svetovni splet svoje prednosti. Poleg tega se lahko predstavljajo hibridne distribucijske oblike, ki kombinirajo spletno distribucijo z različico distribucije brez povezave. Distribucija je le del celovite oskrbovalne verige. Pri e-dobavi je potrebno s pomočjo referenčnega modela uskladiti korake načrtovanja, nabave, proizvodnje in dostave izdelkov in storitev.

Elektronsko plačevanje (e-plačila) omogoča plačevanje majhnih vsot, ki vključujejo le nekaj centov (pikoplačilo), srednjih zneskov v nekaj evrih (mikroplačilo) in večjih zneskov (makroplačilo). Da bi zagotovili, da so transakcijski stroški za pikoplačila in mikroplačila dovolj nizki, da se izplačajo, so bile razvite metode, ki temeljijo na uporabi elektronskih kovancev. Poleg tega obstaja več računskih in lastniških postopkov za elektronska plačila. Da bi zagotovili varnost postopkov elektronskega plačevanja, je treba uporabljati kriptografske postopke in digitalne podpise. Tako na primer SET (varna elektronska transakcija) protokol zahteva uporabo dvojnega postopka podpisa, da so tako podatki o naročilu (v zvezi z trgovcem) kot tudi načini plačila (v zvezi z banko) varovani.

Pri e-upravljanju odnosov s strankami (e-Customer Relationship Management) se osredotočenost na same izdelke premakne k upravljanju s strankami. Poleg običajnih ključnih finančnih kazalnikov je poudarjeno, da je treba zajeti in ovrednotiti stranke, kupce ali na splošno deležnike. Relevantni podatki so shranjeni v skladišču podatkov o strankah, kar omogoča celovito analizo vedenja strank. Poleg analitičnega upravljanja odnosov s strankami uporabljamo tudi večkanalno upravljanje, ki predstavlja poseben izziv, saj je treba oceniti različne komunikacijske kanale s strankami in ugotoviti, kateri so primerni za uporabo. Ta pristop e-poslovanja zahteva največje vložke v realizacijo, vendar lahko zagotovi tudi največje donose. Ti donosi so lahko merjeni v denarju ali pa tudi drugače – na primer v poznavanju vedenja. V zadnjem času so bili vloženi veliki napori; predvsem v EU, v omejevanje zbiranja podatkov/informacij o posameznikih (kupcih) tako s strani posameznih podjetij kot tudi ostalih organizacij (na primer obveščevalnih služb).

3 Informacijska in kibernetska varnosti

Varovanje digitalne pokrajine v hitro spreminjajoči se digitalni dobi, kjer so informacije in podatki v osrčju sodobnega delovanja, se je pomen informacijske varnosti in kibernetske varnosti povzpel na prvo mesto. Ti dve prepleteni disciplini sta namenjeni zagotavljanju razpoložljivosti, celovitosti in zaupnosti digitalnih informacij ter zaščiti posameznikov, organizacij in družb pred razširjenim svetom kibernetskih groženj. (Jereb, 2019) V nadaljevanju je predstavljen splošen pomen kibernetske varnosti v luči načrtovanja in izvajanja digitalizacije poslovanja.

Informacijska varnost obsega strategije, prakse in tehnologije, ki so uvedene za zaščito informacij pred nepooblaščenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem. Vključuje celosten pristop, ki obsega ljudi, procese in tehnologijo. Najpomembnejši ključni vidiki informacijske varnosti vključujejo:

- **razpoložljivost**: zagotavljanje, da so informacije in storitve dostopne in uporabne, kadar je to potrebno.
- **Celovitost**: ohranjanje natančnosti in zaupanja vrednosti podatkov s preprečevanjem nepooblaščenih sprememb.
- **Zaupnost**: zagotavljanje, da so informacije dostopne samo pooblaščenim posameznikom ali entitetam.
- **Avtentikacija in pooblastila**: preverjanje identitete uporabnikov in dodeljevanje ustrezne ravni dostopa.
- **Šifriranje podatkov**: pretvorba podatkov v neberljiv format, da se prepreči nepooblaščen dostop.
- **Upravljanje tveganj/ranljivosti**: identifikacija in naslavljanje ranljivosti, ki bi jih napadalci lahko izkoristili.
- **Usposabljanje zaposlenih**: izobraževanje zaposlenih o najboljših praksah varnosti in potencialnih tveganjih.

Kibernetska varnost se osredotoča na zaščito digitalnih sistemov, omrežij in naprav pred kibernetskimi grožnjami. Te grožnje obsegajo širok nabor zlonamernih dejavnosti, vključno s hekanjem, zlonamerno programsko opremo, izsiljevalsko programsko opremo, prevaro in še več. Ključni elementi kibernetske varnosti vključujejo:

- **varnost omrežja**: zaščita računalniških omrežij pred nepooblaščenim dostopom, vdorom v podatke in drugimi kibernetskimi napadi.
- **Varnost končnih točk**: zavarovanje posameznih naprav (računalnikov, pametnih telefonov, naprav za internet stvari) pred zlonamerno programsko opremo in drugimi kibernetskimi grožnjami.
- **Odziv na incidente**: razvijanje strategij za učinkovit odziv na kibernetske incidente in zmanjšanje njihovega vpliva.
- **Ugotavljanje groženj**: zbiranje in analiziranje informacij o nastajajočih grožnjah, da bi napade predvideli in omilili.
- **Varnostna revizija in spremljanje**: redno ocenjevanje in spremljanje sistemov za znake vdorov ali sumljive dejavnosti.
- **Pravilniki in postopki kibernetske varnosti**: ustvarjanje smernic in protokolov za zagotavljanje doslednih in učinkovitih varnostnih ukrepov.

V današnjem svetu, z medsebojno povezanimi organizacijami različnih tipov in velikosti, se pomembnost informacijske varnosti in kibernetske varnosti ne more precenjevati. Kibernetski napadi imajo potencial, da motijo kritično infrastrukturo, ogrozijo osebne podatke in škodujejo nacionalni varnosti. Izzivi na teh področjih se nenehno razvijajo zaradi naraščajoče kompleksnosti kibernetskih kriminalcev, hitrega napredka tehnologije in vedno številčnejših možnosti za napad.

Pri reševanju informacijske in kibernetske varnosti smo soočeni z izzivi, ki jih skušamo zaobiti z nekaterimi splošno sprejetimi strategijami zato, da bi si zagotovili varno digitalno okolje. Med temi strategijami so najpomembnejši proaktivni in celoviti pristopi, ki jih morajo sprejeti organizacije in posamezniki in vključujejo:

- **izobraževanje in usposabljanje**: neprekinjeno usposabljanje in programi ozaveščanja so ključni, da posameznike pooblastijo za prepoznavanje in odzivanje na kibernetske grožnje.
- **Napredne tehnologije**: sprejemanje tehnologij, kot sta umetna inteligenca in strojno učenje za odkrivanje in preprečevanje kibernetskih groženj v realnem času.
- **Sodelovanje**: deljenje informacij in obveščanje o grožnjah in najboljših praksah med organizacijami (tudi med vladami) za krepitev skupne kibernetske varnosti.

- **Pravila in skladnost s predpisi**: spoštovanje predpisov in standardov za kibernetsko varnost za izboljšanje zaščite podatkov in zasebnosti.
- **Načrtovanje odpornosti**: razvijanje načrtov za odzivanje na incidente in obnovitev delovanja po nesrečah, da se zmanjša vpliv kibernetskih incidentov.

Bolj podroben opis zagotavljanja varnosti pred IT grožnjami in napadi predstavljamo v poglavju o informacijski in računalniški varnosti.

4 Upravljanje IT tveganj in investicij

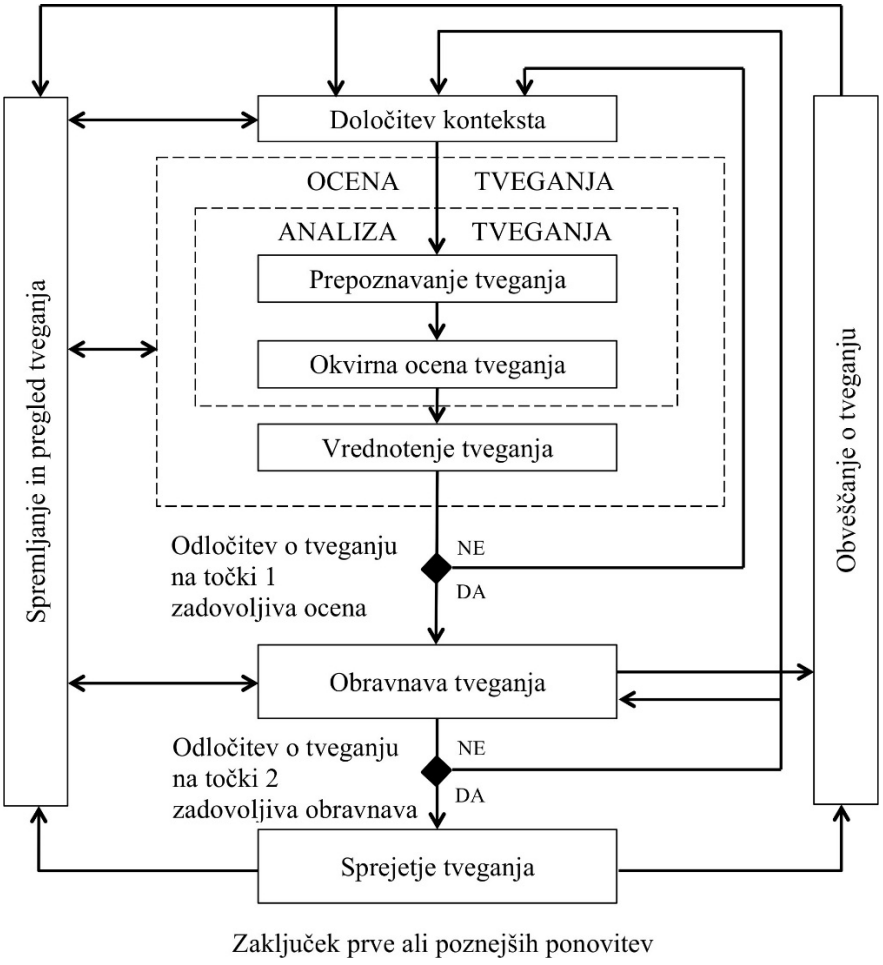
Pri vzpostavitvi sistema upravljanja varnosti morajo organizacije poskrbeti za sistematično upravljanje tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem, v katerem organizacija deluje. Navsezadnje mora biti upravljanje posameznih (operativnih, IT, tečajnih itd.) tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje. Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje s tveganji na področjih, kjer in kadar je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Upravljanje IT tveganj je ključna sestavina celotnega upravljanja tveganj v organizaciji. Vključuje prepoznavanje, ocenjevanje in omilitev tveganj, povezanih z informacijsko tehnologijo, da se zagotovi razpoložljivost, zaupnost in celovitost informacij in sistemov. Ključni vidiki upravljanja tveganj informacijske tehnologije so predstavljeni na Sliki 1.2. Povzeti so po standardu ISO/IEC 27005:2022 (ISO/IEC, 2022), kar je standard, ki opisuje proces upravljanja s tveganji in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost.

Za izvajanje informacijske varnostne politike in sistema varnosti mora biti odgovoren najvišji upravljavski sloj organizacije. Pri tem izvaja proces upravljanja informacijskih tveganj tako, da upošteva kriterij zmanjševanja škode. Zelo groba ocena je, da pri zagotavljanju razpoložljivosti, celovitosti in zaupnosti informacij upošteva poslovni vpliv morebitnega varnostnega incidenta na poslovanje in realno verjetnost, da pride do informacijskega incidenta. (Jereb, 2019)

Ker se tveganjem ni smiselno povsem izogniti, niti se jim ne moremo, se je potrebno z njimi sprijazniti in se jih naučiti upravljati. Pri upravljanju tveganj se vodstva organizacij odločajo o naslednjih možnostih:

- tveganje je potrebno zmanjšati,
- tveganje sprejmemo brez dodatnega ukrepanja,
- tveganju se izognemo,
- tveganje prenesemo na pogodbene ali tretje osebe.



Slika 1.2: Aktivnosti pri upravljanju informacijskih tveganj
Vir: (Jereb, 2019)

Upravljanje informacijskih tveganj po ISO 27005 sestavljajo naslednje aktivnosti, ki jih prikazuje tudi Slika 2:

- **določitev konteksta** v katerem skušamo defnirati okvir za upravljanje tveganj.
- **Oceno tveganja** kjer skušamo ovrednotiti nivo tveganja. Ta sklop vsebuje dve aktivnosti:
  - **analizo tveganja**, ki se ponovno deli na:
    - **prepoznavanje tveganja** in
    - **okvirno oceno tveganja** ter
  - **vrednotenje tveganja**.
- **Obravnava tveganja**, kjer je potrebno sprejeti ustrezne ukrepe tako, da se tveganjem izognemo, jih zmanjšamo, prenesemo na druge ali se odločimo, da jih v danem trenutku sprejmemo takšna, kot so.
- **Sprejetje tveganja**; sprejmemo odločitev za sprejetje ukrepov, povezanih s tveganji in določimo odgovornost za identifkacijo tveganj z utemeljitvami.
- **Obveščanje o tveganjih**, kjer zagotavljamo, da poteka stalna kakovostna izmenjava informacij med vsemi zainteresiranimi javnostmi in upravljavci tveganj o obstoju, naravi, obliki, verjetnosti, resnosti, sprejemljivosti in podobnih dejavnikih tveganj.
- **Spremljanje in pregled**, kjer tveganja in njihove dejavnike spremljamo in pregledujemo, da zaznamo vse spremembe v okviru organizacije ter vzdržujemo celosten vpogled v tveganje.

Praktična uporaba standarda ISO/IEC 27005 v različnih industrijah je ključnega pomena za zagotavljanje robustnega upravljanja IT tveganj. Nekateri hipotetični primeri študij ali primeri, kako bi se lahko ISO/IEC 27005 uporabljal v različnih industrijah, so naslednji.

- Finančni sektor:
  - Scenarij: finančna institucija ali podjetje pri izvajanju finančnih procesov želi izboljšati svoje procese upravljanja tveganj informacijske varnosti.

  - Uporaba: ISO/IEC 27005 se lahko uvede za sistematično prepoznavanje in ocenjevanje tveganj, povezanih s podatki strank, finančnimi transakcijami in skladnostjo s predpisi. Institucija lahko nato izvede prilagojene strategije obvladovanja tveganj za zaščito občutljivih informacij in zagotovitev skladnosti s finančnimi predpisi.
- Zdravstveni sektor:
  - Scenarij: bolnišnica se zanima za varnost zdravstvenih kartonov in medicinskih podatkov.
  - Uporaba: ISO/IEC 27005 ponuja okvir za izvedbo ocenjevanja tveganj glede zaupnosti, celovitosti in razpoložljivosti zdravstvenih podatkov. Bolnišnica ga lahko uporabi za prepoznavanje ranljivosti, ocenjevanje potencialnih kršitev in izvajanje ukrepov za zaščito podatkov pacientov.
- Proizvodni sektor:
  - Scenarij: proizvodno podjetje si prizadeva zavarovati svojo intelektualno lastnino in proizvodne procese.
  - Uporaba: ISO/IEC 27005 lahko pomaga pri oceni tveganj, povezanih s krajo intelektualne lastnine, motnjami v dobavni verigi in prekinitvami operativnosti. Podjetje lahko izvede strategije za zmanjšanje tveganj za zaščito ključnih sredstev in zagotovitev kontinuitete proizvodnih procesov.
- Informacijske tehnologije (IT) storitve:
  - Scenarij: ponudnik IT storitev želi strankam dokazati svojo predanost informacijski varnosti.
  - Uporaba: ISO/IEC 27005 se lahko uporabi za celovito oceno tveganj v portfelju IT storitev. Z identifikacijo in obvladovanjem tveganj, povezanih z vdori v podatke, motnjami v storitvah in kibernetskimi grožnjami, lahko podjetje okrepi svojo verodostojnost in strankam zagotovi predanost informacijski varnosti.
- Vladne agencije:
  - Scenarij: vladna agencija, odgovorna za podatke državljanov, želi okrepiti svoje varnostne ukrepe.
  - Uporaba: ISO/IEC 27005 lahko vodi agencijo pri oceni tveganj, povezanih s tajnostjo podatkov državljanov in razpoložljivostjo ključnih storitev. Agencija lahko razvije in izvede načrte za

obvladovanje tveganj, da zagotovi varno ravnanje s čezmejnimi informacijami.

- Trgovina:
  - Scenarij: trgovina izraža zaskrbljenost glede varnosti podatkov o plačilih strank.
  - Uporaba: ISO/IEC 27005 lahko pomaga trgovski verigi prepoznati tveganja, povezana s procesiranjem plačil, sistemi na prodajnem mestu in spletnimi transakcijami. Z izvajanjem varnostnih kontrol in rednim ocenjevanjem tveganj lahko podjetje zgradi zaupanje strank in zaščiti finančne transakcije.

V vsakem primeru je ključno prilagoditi uporabo ISO/IEC 27005 specifičnim IT tveganjem in zahtevam industrije. To vključuje razumevanje edinstvenih sredstev, groženj in ranljivosti, pomembnih za vsak sektor ter izvajanje učinkovitih strategij za obvladovanje IT tveganj in zmanjšanje potencialnih negativnih vplivov.

Literatura

Meier, A. & Stormer, H. (2009). eBusiness & eCommerce: Managing the Digital Value Chain. Springer Berlin Heidelberg. ISBN 9783540893615

Jereb, B. (2019). *Informatika in informacijska varnost: repetitorij (1. izd)*. Maribor: Univerzitetna založba Univerze. DOI: 10.18690/978-961-286-251-0.

ISO/IEC. (2022). ISO/IEC 27005:2022 - Information technology — Security techniques — Information security risk management. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).