asist. Anja Brelih, mag. inž. mm.
anja.brelih@fgg.uni-lj.si
Univerza v Ljubljani, Fakulteta za gradbeništvo in geodezijo,
Jamova cesta 2, 1000 Ljubljana

doc. dr. Jaka Dujc, univ. dipl. inž. grad.
jaka.dujc@fgg.uni-lj.si
Univerza v Ljubljani, Fakulteta za gradbeništvo in geodezijo,
Jamova cesta 2, 1000 Ljubljana

doc. dr. Robert Klinc, univ. dipl. inž. grad.
robert.klinc@fgg.uni-lj.si
Univerza v Ljubljani, Fakulteta za gradbeništvo in geodezijo,
Jamova cesta 2, 1000 Ljubljana

Strokovni članek
UDK/UDC: 004.056:004.84:69

ANALIZA VARNOSTI IN ZASEBNOSTI OBLAČNIH OKOLIJ ZA BIM
SECURITY AND PRIVACY ANALYSIS OF CLOUD ENVIRONMENTS FOR BIM

Povzetek
Z razvojem in integracijo informacijskega modeliranja gradenj (BIM) in skupnih podatkovnih okolij (CDE) v gradbene projekte se pojavlja tudi potreba po upravljanju varnosti in zasebnosti. Sodelovanje med ponudnikom okolja in uporabnikom zahteva zaupen odnos in spoštovanje standardov. Standard ISO 19650-5 uvaja smernice za varnostno ozaveščen pristop k upravljanju informacij, vendar še vedno ni jasno, kako posamezni ponudniki te smernice upoštevajo. Okolja BIM in CDE vsebujejo občutljive informacije o gradbenih projektih, tako da morata biti varnost in zasebnost prednostna naloga ponudnikov, z izbiro pravega in zaupanja vrednega okolja pa tudi uporabnikov. Pomembno je, da uporabniki ocenijo vsako rešitev in sprejmejo informirano odločitev o tem, komu bodo zaupali svoje podatke. Članek ponuja pregled mehanizmov varnosti in zasebnosti, ki jih je treba upoštevati pri upravljanju informacij in se uporabljajo za zagotavljanje zaupnosti, celovitosti in razpoložljivosti podatkov. Prav tako v članku podamo okvir za zagotavljanje varnosti in zasebnosti, s katerimi se izboljša vidik varnosti in zasebnosti z dosledno obravnavo vseh varnostnih ravni. Priporočilo za ponudnike je, da morajo objaviti jasne in jedrnate informacije o svojih varnostnih politikah in postopkih, za uporabnike pa, da bi morali biti ozaveščeni in konkretni glede lastnih zahtev po varnosti in zasebnosti ter izbrati rešitev, ki ustreza njihovim potrebam.

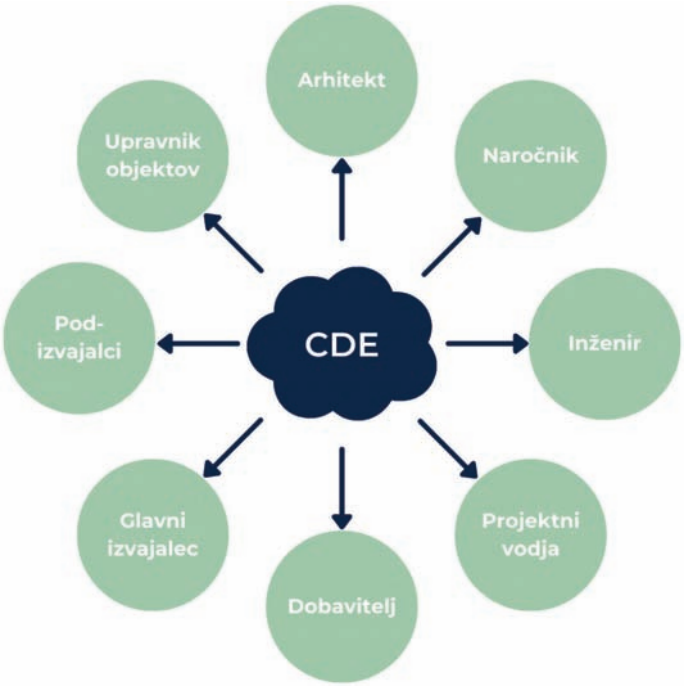
Ključne besede: informacijsko modeliranje gradenj (BIM), skupno podatkovno okolje (CDE), varnost, zasebnost, upravljanje informacij, standardizacija

Summary
With the development and integration of Building Information Modeling (BIM) and Common Data Environments (CDE), the need for security and privacy management also arises in construction projects. Collaboration between the provider of the environment and the user requires a confidential relationship and compliance with standards. ISO 19650-5 guides a security-aware approach to information management, but it is not always clear how individual providers implement these guidelines. The BIM and CDE environments contain sensitive information about construction projects. Therefore, security and privacy should be top priorities for providers and users when choosing the right environment. It has become essential for users to evaluate each solution and make an informed decision about who they trust with their data. The paper provides an overview of the security and privacy mechanisms that should be utilised in information management to ensure the confidentiality, integrity, and availability of data. We also present a framework for ensuring security and privacy that enhances these aspects by systematically addressing all levels of security. Providers should issue clear and concise information about their security policies and procedures, and users should be clear about their own security and privacy requirements and choose a solution that meets their needs.

Key words: building information modeling (BIM), common data environment (CDE), security, privacy, information management, standardization

1 UVOD

Informacijsko modeliranje gradenj (angl. Building Information Modeling, BIM) je proces za ustvarjanje in upravljanje digitalnih predstavitev fizičnih in funkcionalnih značilnosti objektov. Pristop BIM v gradbeništvu postaja vse bolj pomemben, saj povezuje udeležence projekta in ustvarja pregleden potek dela. Da bi v celoti izkoristili funkcionalnosti okolja BIM kot procesa pretoka informacij, moramo vzpostaviti tudi skupno podatkovno okolje (angl. Common Data Environment, CDE) oziroma, z drugimi besedami, infrastrukturo računalništva v oblaku, prikazano na sliki 1. CDE je skupni digitalni delovni prostor, ki projektnim skupinam omogoča sodelovanje ob souporabi vseh projektnih podatkov, tudi modelov BIM.



Slika 1. *Skupno podatkovno okolje (CDE).*

Računalništvo v oblaku je vseprisotna in hitrorastoča računalniška paradigma, ki uporabnikom omogoča dostop do podatkov in aplikacij. Okolja CDE je mogoče implementirati kot infrastrukturo z lokalnim izvajanjem na uporabnikovi lokaciji ali pa se ta izvaja na zunanji lokaciji pri ponudniku oblačnih storitev. Implementacije lahko ustrezajo različnim namestitvenim modelom v oblaku glede na lokacijo, lastništvo in splošno dostopnost. Dva glavna modela sta zasebni in javni oblak. V zasebnem oblaku je lastništvo in upravljanje oblačne infrastrukture v upravljanju podjetja. V nasprotju z zasebnim oblakom je dostop do oblačnih virov pri javnem oblaku odprt za vse. Računalništvo v oblaku ponuja različne modele storitev, ki so specifična, vnaprej pripravljena kombinacija virov informacijske tehnologije (angl. Information technology, IT), ki jih ponuja ponudnik storitev v oblaku in se nanašajo na načine, kako ti ponujajo storitve uporabnikom. Trije glavni modeli storitev so aplikacija kot storitev (angl. Software as a Service, SaaS), platforma kot storitev (angl. Platform as a Service, PaaS) in infrastruktura kot storitev (angl. Infrastructure as a Service, IaaS) [Manvi, 2021]. Skupni digitalni prostori, ki se uporabljajo v gradbeništvu, so običajno ponujeni kot model SaaS v javnem oblaku, kjer uporabniki ne upravljajo in nadzorujejo infrastrukture v oblaku, temveč preprosto uporabljajo rešitve programske opreme v oblaku. V tem primeru so ponudniki komercialnih okoljih CDE odgovorni za upravljanje ter zagotavljanje nadgradenj, vzdrževanja in varnosti.

Eksponentna rast računalništva v oblaku poleg številnih prednosti prinaša vrsto varnostnih vprašanj, ki jih je treba pravilno razumeti in obravnavati za uspešno uporabo rešitev v oblaku [Sun, 2018]. Operacije in podatki v oblaku so povezani s številnimi varnostnimi tveganji, kot so izguba upravljanja, ogrožanje varovanja podatkov, razpoložljivostjo storitev, skladnost in pravno tveganje, neprimerna avtentikacija in avtorizacija itd. Varnost računalništva v oblaku se nanaša na ohranjanje zaupnosti, celovitosti in razpoložljivosti podatkov, shranjenih v oblaku. Varnostne zahteve v oblaku tako vključujejo zanesljivo varnost, zaupanje, zagotovilo, spremljanje in upravljanje [Pavithra, 2019]. Te zahteve je mogoče neposredno prenesti na zahteve glede varnosti in zasebnosti za okolja CDE v oblaku.

Z vse večjim sprejemanjem BIM in CDE postaja potreba po upravljanju varnosti in zasebnosti vse pomembnejša. Ta okolja vsebujejo občutljive informacije o gradbenih projektih, vključno s finančnimi informacijami, intelektualno lastnino in osebnimi podatki. Zato je pomembno, da ponudniki in uporabniki CDE jasno razumejo mehanizme varnosti in zasebnosti, ki so potrebni in se uporabljajo za zaščito teh podatkov.

Problem integracije BIM in računalništva v oblaku so prepoznali že leta 2013 z identifikacijo štirih ravni zaščitnih rešitev, s katerimi je mogoče premagati te izzive: z infrastrukturo, informacijami, pogodbo in ravnmi zaupanja [Mahamadu, 2013]. Te ravni je mogoče neposredno prenesti na zahteve glede varnosti in zasebnosti za okolja CDE v oblaku.

Prispevek v nadaljevanju predstavlja analizo varnosti in zasebnosti oblačnih okolij za BIM. Drugo poglavje ponuja pregled najpogostejših mehanizmov za zagotavljanje varnosti in zasebnosti, ki se uporabljajo v oblačnih okoljih BIM in CDE. V tretjem poglavju je podan pregled standarda ISO 19650-5, ki podaja smernice za varnostno ozaveščen pristop k upravljanju informacij pri uporabi informacijskega modeliranja gradenj. Analiza mehanizmov ponudnikov BIM in CDE je podana v četrtem poglavju. V petem poglavju je predstavljen okvir za zagotavljanje varnosti in zasebnosti v okoljih BIM in CDE, ki omogoča dosledno obravnavo vseh varnostnih ravni in pomaga uporabnikom pri določitvi varnostnih zahtev in izbiri ustreznega ponudnika. Šesto poglavje je namenjeno razpravi, v sedmem poglavju pa so podani zaključki.

2 VARNOSTNI MEHANIZMI V OBLAKU

Z vse večjo uporabo okolij BIM in CDE se povečuje tudi število varnostnih tveganj in groženj, ki jih je treba obravnavati in se pred njimi ustrezno zaščititi. Uporaba mehanizmov za zagotavljanje informacijske varnosti in zasebnosti je ključna za zagotavljanje zaupnosti, celovitosti in razpoložljivosti podatkov v oblaku ter zagotavljanje zaščite pred nepooblaščenim dostopom, izgubo podatkov in grožnjami kibernetski varnosti [Manvi, 2021]:

- **Zaupnost** je preprečevanje namernega ali nenamernega nepooblaščenega razkritja vsebine.
- **Celovitost** je zagotovilo, da sporočilo ni nepričakovano ali namerno spremenjeno.
- **Razpoložljivost** zagotavlja, da je storitev dostopna, ko je to potrebno, kar dovoljuje odobrenim uporabnikom dostop do sistema ali ogrodja (angl. framework).

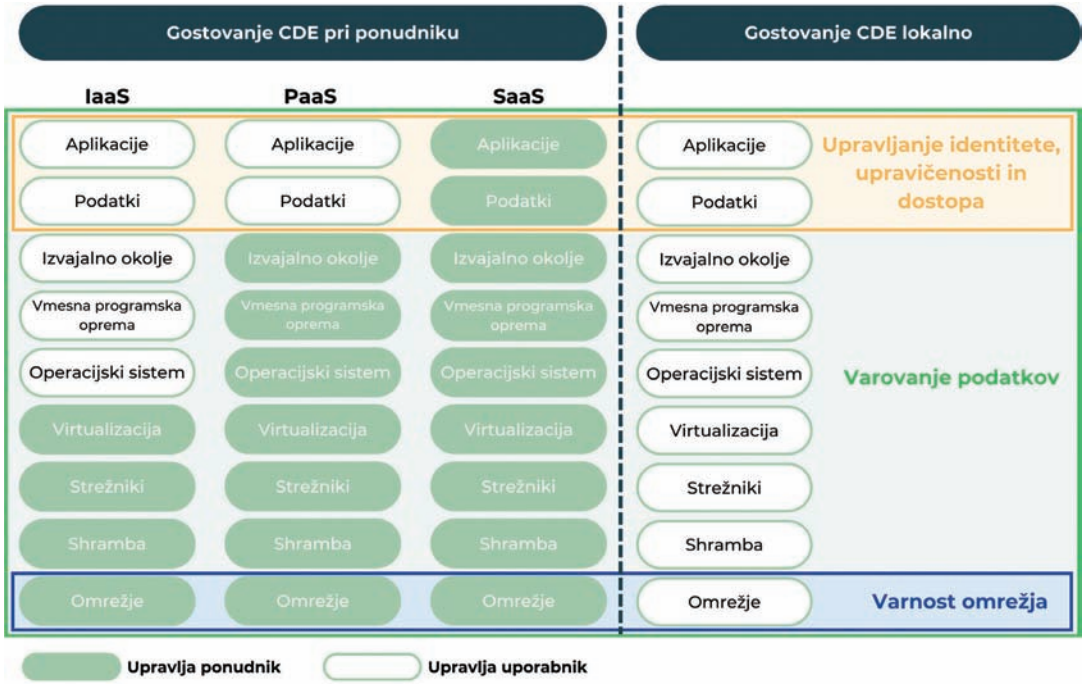
V okoljih CDE, kjer uporabnik običajno uporablja model storitve SaaS, je ponudnik odgovoren za skoraj vso varnost. Uporabnik lahko le dostopa do aplikacije in jo upravlja, nima pa nadzora nad samim delovanjem [CSA, 2021]. Zagotavljanje zasebnosti podatkov je pomemben vidik računalništva v oblaku, saj so občutljivi podatki shranjeni izven domene uporabnika. Z vidika uporabnika se lahko zdi, da je računalništvo v oblaku izpostavljeno varnostnim tveganjem ter pomanjkanju zasebnosti zaradi deljenja virov z drugimi uporabniki ter možnega pomanjkanja nadzora nad svojimi podatki, saj ni vzpostavljenih robustnih varnostnih ukrepov [Bamasoud, 2021]. Ponudniki storitev v oblaku tako uporabljajo različne mehanizme za vzdrževanje varnosti in zasebnosti, da s tem ponujajo zaupanja vredno storitev.

Mehanizme varnosti in zasebnosti računalništva v oblaku je treba upoštevati na več ravneh, da bi uporabnikom zagotovili celovito in zaupanja vredno storitev. V tem prispevku so mehanizmi razdeljeni na varovanje podatkov, varnost omrežja, upravljanje identitete in dostopa, fizično varnost, delitev odgovornosti in skladnost s standardi.

Model odgovornosti za upravljanje različnih plasti okolij v oblaku, prikazan na sliki 2, se razlikuje glede na uporabljeni storitveni model. Varnostni mehanizmi se upoštevajo na vsaki plasti, upravlja pa jih uporabnik ali ponudnik storitve v oblaku. Okolje CDE, ki gostuje na lokalnem strežniku, upravlja uporabnik, ki je tudi lastnik infrastrukture. Pri gostovanju na ponudnikovih strežnikih pa varnost upravlja ponudnik storitve v oblaku.

2.1 Varovanje podatkov

Varovanje podatkov v oblaku se razlikuje od običajne varnosti podatkov zaradi posebne arhitekture shranjevanja. Računalništvo v oblaku običajno uporablja porazdeljeno shranjevanje. Lastništvo in nadzor podatkov sta ločena, kadar uporabljamo CDE, ki gostuje pri ponudniku. Uporabniki so lastniki, nadzor pa imajo ponudniki storitev v oblaku. Varovanje podatkov v oblaku se v glavnem osredotoča na shranjevanje podatkov, prenos in avtentikacijo dostopa ter se večinoma izvaja s šifriranjem [Xu, 2019]. Privzeto so podatki zapisani v človeku berljivi obliki, znani kot čistopis, ki je pri prenosu po omrežju ranljiv za nepooblaščen in potencialno zlonameren dostop. Šifriranje v oblaku je preoblikovanje podatkov uporabnika v tajno obliko z namenom zagotavljanja zaupnosti in celo celovitosti podatkov. Gre za storitev, ki jo ponujajo ponudniki shranjevanja podatkov v oblaku, pri čemer se podatki preoblikujejo z uporabo šifrirnih algoritmov [Manvi, 2021] v zaščiteno in neberljivo obliko, imenovano šifropis. S postopkom šifriranja postanejo podatki neberljivi, če ključa ne poznamo. Postopek šifriranja se lahko izvaja z različnimi tehnikami, kot sta simetrično in asimetrično šifriranje. Pri simetričnem se za šifriranje in dešifriranje uporablja isti ključ, pri asimetričnem pa se uporablja par javnega in zasebnega ključa. Za simetrično šifriranje obstaja več algoritmov, med katerimi se najpogosteje uporabljata napredni šifrirni standard (angl. Advanced Encryption Standard, AES) in standard za šifriranje podatkov (angl. Data Encryption Standard, DES) oziroma njegova različica trojni DES (angl. Triple DES). Najbolj znan predstavnik asimetričnega šifriranja oziroma šifriranja z javnim ključem je algoritem RSA, poimenovan po svojih kreatorjih Rivest, Shamir in Adleman. Pomemben vidik varovanja podatkov med prenosom ali oddaljenem shranjevanju je ohranjanje njihove celovitosti. V ta namen se



Slika 2. *Model odgovornosti za mehanizme informacijske varnosti glede na storitvene modele v oblaku.*

lahko uporabljajo zgoščevalne funkcije, ki zagotavljajo, da so prejeti podatki identični originalnim. V praksi se najpogosteje uporabljata 256-bitni algoritem varnega zgoščevanja (angl. Secure Hash Algorithm 256-bit, SHA-256) ter algoritem izvlečka besedila 5 (angl. Message Digest Algorithm 5, MD5).

2.2 Varnost omrežja

Varnost omrežja zajema zaščito podatkov, ko prečkajo omrežja, kot je internet, zaščito sistemov in podatkov pred omrežnimi napadi ter zaščito samih omrežnih komponent. Ponudnik storitev v oblaku lahko zagotovi varnost omrežnega okolja uporabnikom tako, da ponuja storitve v oblaku, ki zagotavljajo šifriranje prometa, spremljanje omrežja, analizo in nadzor prometa, navidezna zasebna omrežja (angl. Virtual Private Networks, VPN), požarne zidove in varne omrežne storitve [CSA, 2012].

2.3 Upravljanje identitete, upravičenosti in dostopa

Računalništvo v oblaku močno vpliva na upravljanje identitete in dostopa (angl. Identity and Access Management, IAM). V javnem in zasebnem oblaku morata dve strani upravljati IAM brez ogrožanja varnosti. Računalništvo v oblaku uvaja številne spremembe v načinu upravljanja dostopa do notranjih sistemov. Ključna razlika je odnos med ponudnikom in uporabnikom oblaka. IAM ne more upravljati samo eden ali drugi, zato sta potrebna zaupni odnos in določitev odgovornosti, ki omogočata upravljanje identitete, upravičenosti in dostopa [CSA, 2012]. Obstaja več standardov za upravljanje identitete in dostopa, ki se uporabljajo v računalništvu v oblaku. Po navedbah [CSA, 2021] med najbolj razširjene standarde za preverjanje identitete spadajo SAML (angl. Security Assertion Markup Language), Oauth 2.0 in OpenID, ki spadajo pod enotno prijavo (angl. Single Sign-On, SSO).

2.4 Fizična varnost

Pomembno vlogo pri zagotavljanju varnostnih mehanizmov v oblaku ima tudi zagotavljanje fizične varnosti strežniške infrastrukture. Mehanizmi za zagotavljanje fizične varnosti vključujejo različne nivoje kontrole in ukrepov za nadzorovanje dostopa in aktivnosti. Za zagotavljanje te ravni varnosti je odgovoren ponudnik oblačnih storitev, ki ima nadzor nad fizično infrastrukturo. Zagotoviti mora varnost tako pred fizičnimi napadi kot pred naravnimi nesrečami in izpadi električne energije. Vsak vidik podatkovnega centra, od lokacije in dostopnosti do gostote moči in redundance, mora biti zasnovan tako, da zagotavlja njegovo varnost, odpornost in učinkovitost. Podatkovni centri so varovani objekti, do katerih imajo fizični dostop samo pooblaščene osebe, ki jih nadzorujejo s kamerami in varujejo varnostniki, da odkrijejo možne sumljive dejavnosti in jih preprečijo.

Kljub temu lahko pride do incidentov zaradi naravne nesreče, fizičnega napada ali kibernetskega napada. Zato je pomembno, da so ponudniki storitev v oblaku pripravljeni na takšne dogodke in da imajo vzpostavljene mehanizme za obnovitev po nesreči in zagotavljanje poslovne kontinuitete. Varnostno kopiranje podatkov, shranjenih v oblaku, ima pomembno vlogo v primeru odpovedi sistema in potrebe po obnovitvi pomembnih podatkov. Pri vpeljevanju varnostnega kopiranja podatkov se uvajajo različne strategije, kot so popolne varnostne kopije, inkrementalne in diferencialne varnostne kopije. Glede na pomembnost in občutljivost podatkov, shranjenih v oblaku, je treba razmisliti, kateri pristop za varnostno kopiranje je smiselno uporabiti.

2.5 Model deljene odgovornosti

Cloud Security Alliance [CSA, 2021] identificira tako imenovani model deljene odgovornosti, ki je neposredno povezan z dvema priporočiloma za varnost aplikacij v oblaku:

1. Ponudniki oblaka morajo jasno dokumentirati svoje notranje varnostne kontrole in varnostne funkcije strank, da lahko uporabnik oblaka sprejme informirano odločitev. Ponudniki bi morali te kontrole tudi ustrezno oblikovati in izvajati.

2. Uporabniki oblaka bi morali ustvariti matriko odgovornosti za vsak posamezen projekt, da bi dokumentirali, kdo izvaja katere kontrole in kako.

Model deljene odgovornosti navaja, da sta pri obravnavi tehnologije računalništva v oblaku vpleteni dve strani, ki sta odgovorni za izvajanje in upravljanje različnih delov sklada (angl. stack). Za ta odnos je ključnega pomena zaupanje.

Analiza obstoječe literature o zaupanju pri projektih identificira tri različne pristope k preučevanju zaupanja [Cerić, 2021], in sicer psihološko, sociološko in ekonomsko. Psihološki pristop se osredotoča na dinamiko zaupanja, medtem ko sociološki pristop preučuje zaupanje znotraj skupin in organizacij. Ekonomski pristop na drugi strani analizira, kako zaupanje vpliva na ekonomske interakcije. Ključni dejavniki, ki prispevajo k zaupanju v tovrstne projekte, so učinkovita komunikacija, transparentnost, ugled in trdni odnosi.

Zaupanje je pomemben vidik gradbenih projektov in velja tudi za sodelovanje vseh strani, ki uporabljajo ali zagotavljajo oblačna okolja CDE. Za uspešno implementacijo teh rešitev je pomemben zaupen odnos, tako da ponudniki in uporabniki urejajo ter spoštujejo aktivnosti modela deljene odgovornosti, ki se nanaša na varnost oblačnih okolij.

2.6 Skladnost z varnostnimi standardi

Poleg serije standardov ISO 19650 ([SIST, 2019a], [SIST, 2019b], [SIST, 2020a], [SIST, 2020b], [SIST, 2023]), ki urejajo področje upravljanja informacij pri uporabi informacijskega modeliranja gradenj, morajo okolja CDE izpolnjevati tudi standarde, ki veljajo za računalništvo v oblaku. V zadnjem desetletju je vse več sredstev in prizadevanj namenjenih boju proti kibernetskim grožnjam v oblačnih okoljih. Za učinkovito merjenje ravni varnosti, ki jo zagotavljajo ponudniki storitev v oblaku, je potrebna standardizacija postopkov potrjevanja in certificiranja. Standardi temeljijo na merljivih indikatorjih, ki jih predstavljajo kontrole, kot je kontrolni seznam, ali splošne, a nedvoumne zahteve, kot so klavzule ali načela [Di Giulio, 2017].

Standardi računalništva v oblaku se nenehno razvijajo, zato je pomembno, da ponudniki in uporabniki storitev v oblaku spremljajo najnovejše standarde in tako zagotovijo, da so njihova okolja v oblaku varna in skladna. Družina standardov ISO/IEC 27000 velja za najbolj razširjene standarde za sisteme upravljanja informacijske varnosti in njihove zahteve.

Organizacijam omogočajo upravljanje varnosti sredstev, kot so finančne informacije, intelektualna lastnina, podatki zaposlenih in informacije, zaupane tretjim osebam [ISO, 2018]. Standard ISO/IEC 27001 vsebuje navodila za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja informacijske varnosti. Skladnost s standardom ISO/IEC 27001 pomeni, da je organizacija ali podjetje vzpostavilo sistem za obvladovanje tveganj, povezanih z varnostjo podatkov, ki jih hrani ali obdeluje, in da je ta sistem skladen z vsemi najboljšimi praksami in načeli, opisanimi v tem mednarodnem standardu [ISO, 2022a]. Poleg skladnosti s standardom ISO/IEC 27001 je treba upoštevati tudi skladnost s standardom ISO/IEC 27017, ki ponuja nadaljnjo usmeritev na področju informacijske varnosti računalništva v oblaku [ISO, 2015]. ISO/IEC 27017 dopolnjuje priporočila standarda ISO/IEC 27002 [ISO, 2022b] in različnih drugih standardov iz družine ISO/IEC 27000, kot sta ISO/IEC 27018 o vplivu računalništva v oblaku na zasebnost, ki se osredotoča na zaščito osebnih podatkov (angl. Personally identifiable information, PII) v javnih oblakih, ki služijo kot procesorji PII ([ISO, 2019], [ISO, 2022a]) in standard ISO/IEC 27031 o neprekinjenem poslovanju [ISO, 2011].

Revizije storitev in organizacije 2 (angl. Service and Organization Audits 2, SOC 2) se ukvarja z revizijo operativnih procesov, ki jih uporabljajo podjetja IT, ki ponujajo katerokoli storitev, in velja za svetovni standard za sisteme za obvladovanje tveganj kibernetske varnosti. Politike, prakse in nadzor podjetja so vzpostavljeni za izpolnjevanje petih načel zaupanja (varnost, razpoložljivost, celovitost obdelave, zaupnost in zasebnost), ki so ocenjevani v revizijskem poročilu [GeeksforGeeks, 2023].

3 STANDARD ISO 19650

Serija standardov ISO 19650 »*Organizacija in digitalizacija informacij o gradnjah in gradbenih inženirskih delih, vključno z informacijskim modeliranjem gradenj – Upravljanje informacij z uporabo informacijskega modeliranja gradenj*« je mednarodni standard za upravljanje informacij v celotnem življenjskem ciklu grajenega sredstva z uporabo BIM [BSI, 2023]. Serija je razdeljena na pet delov:

1. **Pojmi in načela (angl. Concepts and principles)**: pregled načel in konceptov upravljanja informacij z uporabo BIM [SIST, 2019a].
2. **Faza načrtovanja in izvedbe gradbenega projekta (angl. Delivery phase of the assets)**: zahteve za upravljanje informacij v fazi dostave grajenega sredstva, od načrtovanja in projektiranja do gradnje [SIST, 2019b].
3. **Obratovalna faza sredstev projekta (angl. Operational phase of the assets)**: zahteve za upravljanje informacij v operativni fazi zgrajenega sredstva, od predaje do vzdrževanja in rušenja [SIST, 2020a].
4. **Izmenjava informacij (angl. Information exchange)**: zahteve za izmenjavo informacij BIM med različnimi programskimi aplikacijami in deležniki [SIST, 2023].
5. **Varnostni pristop k upravljanju informacij (angl. Security-minded approach to information management**: zahteve za upravljanje varnosti informacij v projektih BIM [SIST, 2020b].

Standard ISO 19650-5 »*Varnostni pristop k upravljanju informacij*« z uporabo BIM zagotavlja okvir, ki organizacijam pomaga razumeti ključne ranljivosti in vrsto nadzora potrebnega za omejitev varnostnih tveganj na raven, ki je sprejemljiva za vse deležnike. Standard prepoznava, da uporaba računalniških tehnologij že podpira nove načine dela, vendar je treba upoštevati pripadajoče ranljivosti in posledična varnostna tveganja. Standard spodbuja sprejetje varnostno naravnanega pristopa, ki temelji na tveganju in ga je mogoče uporabiti tako znotraj kot zunaj organizacije. Dokument je namenjen vsem organizacijam, ki sodelujejo pri uporabi upravljanja informacij in tehnologij pri vseh dejavnostih, povezanih z grajenimi sredstvi ali proizvodi in zagotavljanjem storitev v grajenem okolju [ISO, 2020]. Glavni del standarda ISO 19650-5 je razdeljen na šest poglavij:

1. **Ugotavljanje potrebe po varnostno naravnanem pristopu z uporabo postopka ocenjevanja občutljivosti.** To poglavje opisuje varnostna tveganja, ugotavljanje občutljivosti organizacije, ugotavljanje občutljivosti tretjih oseb, beleženje in pregled ocenjevanja. V poglavju je opisan postopek ugotavljanja, ali je varnostno naravnan pristop sploh potreben, opredeljene so potrebe po zapisovanju izida postopka varnostnega pregleda in navedena navodila, ki jih je treba upoštevati, če je varnostno naravnan pristop potreben.
2. **Začetek varnostno naravnanega pristopa.** Navaja navodila za vzpostavitev upravljanja in odgovornosti ter začetek razvoja za pristop glede sodelovanja znotraj organizacije ter med več organizacijami. Poudarjeno je, da mora opisane dejavnosti za izvajanje pristopa opravljati ustrezno usposobljena in izkušena oseba.
3. **Razvoj varnostne strategije.** Pojasnjuje, kaj je treba vključiti v varnostno strategijo. Vključena so tudi navodila, kako oceniti varnostna tveganja in razviti omilitvene ukrepe z ustrezno dokumentacijo in načrtom pregleda.
4. **Razvoj načrta za upravljanje varnosti.** Navaja vse, kar mora biti vključeno v varnostni načrt ter navodila za posredovanje informacij tretjim osebam, kar vključuje navodila za spremljanje, revidiranje in pregledovanje načrta upravljanja varnosti ter upravljanje odgovornosti za varnost.
5. **Razvoj načrta za obvladovanje kršitev varnosti oziroma incidentov.** Vsebuje navodila za ravnanje ob morebitni kršitvi varnosti ali incidentu ter informacije o tem, kako izdelati načrt, ki vključuje odkrivanje in obvladovanje incidenta, okrevanje in pregled po njemu.
6. **Sodelovanje z imenovanimi strankami.** Zadnje poglavje vsebuje navodila za delo zunaj uradnih imenovanj (npr. pri javnih razpisih) in ukrepih iz dokumentov o imenovanju, pri katerih bodo naleteli na občutljive informacije.

Standard vključuje tudi štiri priloge z informacijami o (1) varnostnem kontekstu, (2) vrstah kadrovskih, fizičnih in tehničnih varnostnih kontrol ter upravljanju informacijske varnosti, (3) oceni v zvezi z zagotavljanjem informacij tretjim osebam in (4) sporazumih o izmenjavi informacij. Priloge vsebujejo dodatne informacije o varnosti občutljivih informacij in pomagajo vpletenim stranem pri določanju pristopa.

4 OCENA VARNOSTI IN ZASEBNOSTI PONUDNIKOV BIM IN CDE

Z razširjeno uporabo okolij BIM in CDE v gradbenih projektih se povečuje tudi število orodij, ki ta okolja ponujajo. Ponudniki CDE za zagotavljanje storitev končnim uporabnikom uporabljajo infrastrukturo računalništva v oblaku in morajo zagotoviti mehanizme za varnost in zasebnost, opisane v drugem

poglavju, da zagotovijo zaupnost, celovitost in razpoložljivost. Preglednica 1 prikazuje oceno teh mehanizmov za ponudnike oziroma storitve Dalux ([Dalux, 2020], [Dalux, 2023a], [Dalux, 2023b]), Procore ([Procore, 2023a], [Procore, 2023b]), Autodesk BIM360 [Autodesk, 2022] in Trimble ([Trimble, 2023a], [Trimble, 2023b]) na podlagi javno dostopnih informacij.

Na podlagi zbranih informacij lahko ugotovimo, kako izbrani ponudniki CDE ravnajo z občutljivimi podatki uporabnikov. Ponudnika Procore in Autodesk zagotavljata potrebne podatke o svojih varnostnih mehanizmih, Dalux in Trimble pa ponujata le delne informacije.

		Dalux	Procore	Autodesk BIM360	Trimble
Varovanje podatkov	Šifriranje	**	Shranjeni podatki so šifrirani. **	Shranjeni podatki so šifrirani z AES-256.	*
	Zgoščevanje podatkov	Funkcije Argon2, BCrypt, PBKDF2 ipd. se uporabljajo za gesla.	*	Soljena zgoščena vrednost (angl. Salted hash) gesel.	*
Varnost omrežja	Požarni zid	*	✓	✓	*
	Varnost prenosnega sloja (angl. Transport Layer Security, TLS)	✓	TLS v1.2 z 256-bitnim šifriranjem.	TLS v1.2 z varnimi šiframi.	*
IAM	Avtentikacija	✓**	Enotna prijava s SAML. OAuth 2.0 API avtentikacija z aplikacijami tretjih oseb.	Enotna prijava.	Enotna prijava.
	Avtorizacija	✓**	Dostop na podlagi vlog.	Dostop na podlagi vlog.	**
Fizična varnost	Lokacija	Uporablja Amazon Web Services EMEA SARL.	16 varnih globalnih lokacij za shranjevanje datotek. Zasebna infrastruktura v oblaku za podatke v mirovanju.	Vsi podatki so shranjeni v varovanih podatkovnih centrih, ki so v lasti in upravljanju Amazon Web Services.	Uporablja Amazon Web Services.
	Varnostno kopiranje	Dnevno varnostno kopiranje podatkov.	Redundantna infrastruktura z več replikami aplikacijske programske opreme na vsakem strežniku. Vsi podatki se vsakih 20 minut kopirajo v shrambo zunaj spletnega mesta.	Podatki se replicirajo med podatkovnimi centri na ločenih lokacijah. Replikacija preprečuje možnost izgube podatkov ali zamude pri storitvi. Podatki se običajno replicirajo v 15 minutah.	**
	Razpoložljivost	**	99,9% neprekinjenega delovanja.	Visoka razpoložljivost z redundantnimi sistemi.	99,98% neprekinjenega delovanja.
Skladnost s standardi	SOC 2	*	Skladni s standardom SOC 2 (tip 2).	Skladni s standardom SOC 2 (tip 2).	Skladni s standardom SOC 2 (tip 2).
	ISO 19650	*	*	*	*
	ISO 27000	Ponudnik storitev gostovanja je skladen z ISO 27001 (ali enakovrednim standardom).	Skladni z ISO 27001:2013 [ISO, 2013].	Skladni z ISO 27001, ISO 27017 in ISO 27018.	Skladni z ISO 27001:2013 [ISO, 2013].

* Informacije niso podane.
** Informacije so podane, a nejasne.

Preglednica 1. *Ocena varnosti in zasebnosti ponudnikov BIM in CDE.*

Mehanizmi za *varovanje podatkov*, zlasti šifriranje, so izrecno navedeni le pri ponudniku storitve BIM360. Drugi ponudniki navajajo le, da zagotavljajo šifriranje. Podobno le Autodesk in Procore zagotavljata ustrezne informacije za *varnost omrežja* in *IAM*.

Fizična varnost je odvisna od tega, ali ponudniki CDE najemajo kapacitete pri tretjih ponudnikih ali imajo lastno infrastrukturo v oblaku. Ker uporabniki gostijo svoje podatke v aplikaciji, morajo imeti informacije o tem, kje in kako so njihovi podatki shranjeni, kakšna je razpoložljivost in kakšne metode varnostnega kopiranja se uporabljajo. To je še posebej pomembno v Evropski uniji, kjer zasebnost podatkov ureja Splošna uredba o varstvu podatkov (GDPR). Ponudnika Procore in Autodesk končnim uporabnikom zagotavljata dovolj informacij, medtem ko Dalux in Trimble ne zagotavljata potrebnega vpogleda.

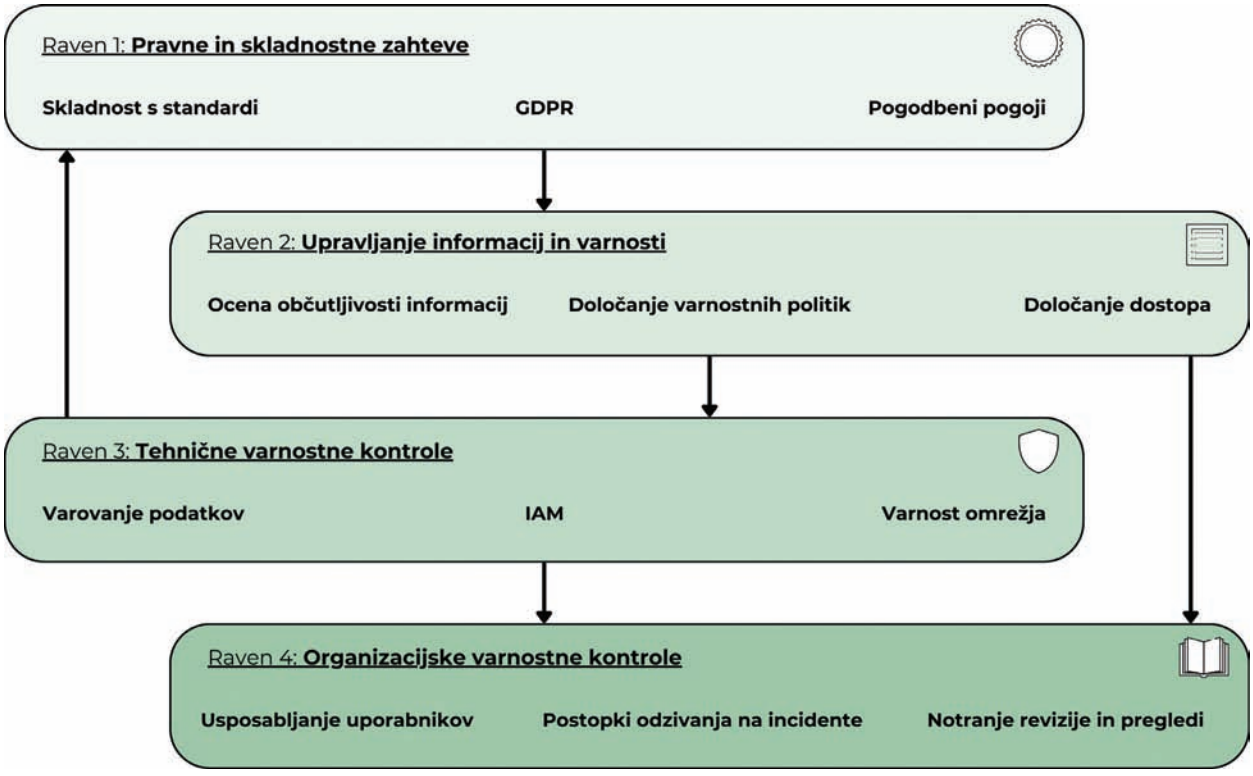
Pri izbranih ponudnikih smo preverili skladnost s standardi, ki veljajo za okolja računalništva v oblaku in BIM. Vsi razen storitve Dalux navajajo skladnost s standardom SOC 2. Izbrani ponudniki so prav tako skladni vsaj s standardom ISO 27001 za sisteme upravljanja informacijske varnosti iz družine standardov ISO 27000. Samo storitev BIM360 je skladna z ISO 27017 in ISO 27018, ki vsebujeta smernice za upravljanje informacij v okoljih računalništva v oblaku. Nobeno od izbranih orodij pa se ne sklicuje na skladnost s standardom ISO 19650, ki ureja upravljanje informacij pri uporabi BIM.

5 OKVIR ZA ZAGOTAVLJANJE VARNOSTI IN ZASEBNOSTI V OKOLJIH CDE

Digitalizacija gradbenih procesov in uporaba oblačnih rešitev v informacijskem modeliranju prinašata nova tveganja na področju kibernetske varnosti, pri čemer je pri sodobnih (na oblačnih storitvah temelječih) modelih treba biti pozoren na vse vidike varnosti in zasebnosti. Veliko težavo predstavlja dejstvo, da gre med lastnikom podatkov ter ponudnikom storitve za poslovni odnos, pri čemer se tako tehnični kot tudi pravni, varnostni in zasebnostni vidiki medsebojnega odnosa pogosto zanemarijo. To je še posebej težavno zato, ker varnost ni statičen koncept, temveč se nenehno spreminja. Zato je ključnega pomena, da organizacije redno preverjajo in prilagajajo svoje varnostne ukrepe, da bi ostale korak pred vedno bolj sofisticiranimi kibernetskimi grožnjami.

Ker okolja BIM in CDE vsebujejo veliko občutljivih informacij, je treba vzpostaviti okvir za učinkovito varovanje teh okolij.

Okvir je strukturiran model, ki združuje upravljavske, tehnične, organizacijske in pravne vidike za zagotavljanje varnosti in zasebnosti v okoljih BIM in CDE (slika 3). Predlagani okvir zagotavlja celovit pristop k obvladovanju varnosti in zasebnosti v okviru BIM-pristopa, ki temelji na centralnem CDE. Skladnost s priporočili in redni varnostni pregledi povečujejo odpornost projektov proti kibernetskim grožnjam ter prispevajo k varnemu digitalnemu delovnemu okolju.



Slika 3. *Okvir za zagotavljanje varnosti in zasebnosti v okoljih BIM in CDE.*

Okvir temelji na štirih ravneh, pri čemer vsaka zagotavlja dosledno postavitev in vzdrževanje varnostnih ukrepov v oblačnih okoljih BIM in CDE.

Prva raven, ki vključuje **pravne in skladnostne zahteve**, zajema skladnost z varnostnimi standardi za oblačna okolja, varnostne pristope k upravljanju informacij ter zaščito podatkov. Te zahteve morajo biti pri izvedbi projekta določene kot pogodbene obveznosti ponudnika oblačne storitve. Skladnost s standardi, kot so ISO/IEC 27001 in ISO/IEC 27017, ter upoštevanje zakonodaje, kot je GDPR, zagotavljata, da so vsi postopki in politike prilagojeni zakonodajnim zahtevam in najboljšim praksam, kar je ključno za ohranjanje zaupanja in zaščito občutljivih informacij.

Druga raven, **upravljanje informacij in varnosti**, vključuje oceno občutljivosti informacij, določanje varnostnih politik ter upravljanje dostopa do občutljivih informacij. Ta raven se izvaja na ravni organizacije, ki izvaja projekt, in mora v začetnih fazah oceniti in definirati varnostna tveganja. Dosledna implementacija prve ravni je osnova za uvedbo naslednjih ravni ter zagotavljanje celotne varnosti in zasebnosti projekta, ki se izvaja v oblačnih okoljih BIM in CDE. Ključni elementi tega procesa so identifikacija morebitnih groženj, ocena tveganj in priprava strategij za njihovo obvladovanje, kot so šifriranje podatkov, nadzor dostopa ter segmentacija omrežij, kar prispeva k večji odpornosti pred kibernetskimi napadi. Ukrepanje na prvi ravni služi kot temelj za implementacijo tehničnih varnostnih kontrol na naslednji stopnji.

Na ravni **tehnične varnostne kontrole** se določajo varnostni mehanizmi, ki so nujni za zagotavljanje varnosti in zasebnosti v oblačnih okoljih. Ta tretja raven vključuje specifikacije, ki jih mora izpolnjevati ponudnik oblačnih storitev, kot so šifriranje podatkov, požarni zidovi, zaščita omrežij in sistemi za upravljanje identitet in dostopa (IAM). Druga raven je tesno povezana z modelom deljene odgovornosti, saj določa, kateri varnostni ukrepi so odgovornost ponudnika in kateri uporabnika. Posebna pozornost je namenjena varnemu shranjevanju in prenosu podatkov, kjer uporaba naprednih tehničnih rešitev, kot so večfaktorska avtentikacija in napredni požarni zidovi, igra ključno vlogo pri zmanjševanju tveganj.

Četrta raven, raven **organizacijske varnostne kontrole**, se nanaša na notranje kontrole, ki služijo za vzdrževanje varnosti in zasebnosti med izvajanjem projekta. To vključuje redno usposabljanje uporabnikov o varnostnih tveganjih, razvoj načrtov za odzivanje na incidente in izvajanje varnostnih testov. Zelo pomembno je, da se uporabniki zavedajo svoje vloge pri varovanju podatkov in se znajo pravilno odzvati na morebitne varnostne incidente, s čimer se izboljša celotna varnostna kultura v organizaciji.

Pri tem je treba posebej opozoriti, da gre pri predlaganem okviru za dinamičen iterativen proces. Vse ravni predlaganega okvira so med sabo neločljivo povezane in jih je treba obravnavati celovito. Pri tem se aktivnosti na posameznih ravneh delijo na:

- **Operativne aktivnosti.** Te aktivnosti se izvajajo za vsak projekt posebej in se prilagajajo strateškim usmeritvam. Med njih sodijo:
  - ocena občutljivosti informacij,
  - določanje varnostnih politik,
  - določanje dostopa,
  - postopki odzivanja na incidente,
  - pogodbeni pogoji itd.
- **Strateške aktivnosti.** Trajnost rezultatov teh aktivnosti je daljša in je večinoma odvisna od zunanjih dejavnikov, kot sta denimo nacionalna ali evropska zakonodaja ter standardi, priporočila in smernice za vzpostavljanje in vzdrževanje informacijske varnosti in zasebnosti oblačnih okolij.

6 DISKUSIJA

ISO 19650-5 je pomemben standard, ki zagotavlja okvir za informacijsko varnost pri upravljanju informacij z uporabo BIM. Vendar pa obstaja nekaj kritičnih področij, pri katerih bi bilo mogoče standard izboljšati.

Eno od glavnih področij za izboljšave je osredotočenost standarda na kibernetsko varnost. Standard se trenutno osredotoča na splošno informacijsko varnost, posebej pa ne obravnava tveganj, ki jih predstavlja internet, npr. kibernetskih napadov, zlorabe podatkov in zlonamerne programske opreme. Ta vidik je pomemben, saj so projekti BIM vse bolj odvisni od tehnologij računalništva v oblaku, ki so po naravi izpostavljene internetnim grožnjam.

Drugo področje, ki ga je treba izboljšati, je jasnost in doslednost standarda. Na nekaterih področjih je standard nejasen ali dvoumen. To lahko organizacijam otežuje izpolnjevanje zahtev standarda. Standard bi moral vključevati bolj specifična in jasna navodila za vse strani, ki so vključene v proces BIM.

Nazadnje bi lahko standard vseboval podrobnejša navodila za izvajanje varnostnih ukrepov. Standard sicer vsebuje nekaj splošnih navodil, vendar ne vsebuje posebnih priporočil za postopke ali orodja in se ne osredotoča na tehnologije v oblaku, ki se uporabljajo v podporo BIM in omogočajo CDE.

Standard bi moral opisati povezavo med ponudniki BIM in CDE ter organizacijami, ki uporabljajo njihove storitve. Z jasnimi opredelitvami tehničnih vidikov informacijske varnosti in zasebnosti v standardu bi lahko organizacije bolje pripravile svoj varnostno usmerjeni pristop. Tehnične zahteve bi bile lahko navedene v prilogi B, ki vsebuje informacije o vrstah kadrovskega, fizičnega in tehničnega varnostnega nadzora ter upravljanja informacijske varnosti. Izboljšanje standarda ne bi pomagalo le organizacijam, ki uporabljajo BIM, temveč tudi ponudnikom teh okolij, ki niso vedno transparentni glede svojih varnostnih mehanizmov.

Ponudniki BIM in CDE morajo upoštevati standarde za informacijsko varnost in zasebnost, zlasti tiste, ki so namenjeni okoljem računalništva v oblaku, npr. standard ISO 27017. Glede na občutljivost informacij v gradbenih projektih si morajo ta okolja prizadevati, da uporabnikom zagotovijo čim bolj varno in zanesljivo storitev. Vse ponudnike bi bilo treba spodbujati, da uporabnikom razkrijejo svoje varnostne mehanizme, tako da lahko ustrezno ocenijo, ali storitev izpolnjuje njihove varnostne potrebe, in imajo možnost oceniti morebitne ranljivosti pri uporabi njihove storitve.

Tehnične zahteve za varnost informacij in zasebnost bi morale postati bistveni del načrta za izvedbo BIM-pristopa (angl. BIM Execution Plan, BEP), ustreznega ponudnika CDE pa bi bilo treba izbrati tudi na podlagi varnostnih zahtev projekta. Pri tem igra ključno vlogo okvir za zagotavljanje varnosti in zasebnosti v okoljih BIM in CDE, saj ponuja celovit pristop k obvladovanju varnostnih tveganj. Okvir združuje različne ravni, od upravljanja informacij in varnosti, tehničnih varnostnih kontrol, organizacijskih varnostnih ukrepov do pravnih in skladnostnih zahtev, kar omogoča, da so vsi varnostni vidiki projekta sistematično obravnavani. Uporaba tega okvira kot osnove za pripravo BEP in za izbiro ponudnika CDE zagotavlja, da se varnostne zahteve upoštevajo že v zgodnjih fazah projekta, kar povečuje odpornost proti kibernetskim grožnjam ter izboljšuje zaščito občutljivih informacij skozi celoten življenjski cikel gradbenega projekta.

7 SKLEP

Vse pogostejša uporaba BIM in CDE v gradbenih projektih zahteva zanesljive varnostne mehanizme za zaščito občutljivih informacij o projektu. Ta prispevek vsebuje pregled ključnih mehanizmov za upravljanje informacij ter skupnih tehnologij in standardov, ki se uporabljajo za zagotavljanje zaupnosti, celovitosti in razpoložljivosti podatkov.

Naš pregled izbranih ponudnikov CDE je razkril nedosledno raven podanih informacij glede mehanizmov varnosti in zasebnosti. Medtem ko nekateri ponudniki, kot sta BIM360 in Procore, ponujajo jasne in natančne informacije o varnostnih politikah, drugi javno objavljajo le delne ali nepopolne podrobnosti. Zaradi pomanjkanja preglednosti uporabniki težko sprejemajo informirane odločitve o izbiri ustreznega okolja CDE.

Čeprav smo se osredotočili na glavne vidike varnosti računalništva v oblaku, se je treba zavedati, da na delovanje storitev v oblaku vplivajo tudi številni drugi dejavniki, vključno s penetracijskim testiranjem in upravljanjem incidentov. Oboje ima ključno vlogo pri zagotavljanju kibernetske varnosti in neprekinjenega poslovanja.

BIM in CDE morata kot aplikaciji računalništva v oblaku upoštevati standarde varnosti in zasebnosti informacij v okolju oblaka. Glede na to, da gre za občutljive informacije, pa ponudniki CDE potrebujejo dodatne spodbude za zagotavljanje varnih rešitev, ki so posebej prilagojene gradbeništvu. Standard ISO 19650-5 bi moral določiti jasne zahteve za ponudnike in uporabnike CDE, pri čemer bi morale biti posebne zaveze vključene v BEP. V tem kontekstu okvir za zagotavljanje varnosti in zasebnosti v okoljih BIM in CDE ponuja strukturiran pristop, ki omogoča dosledno obravnavo vseh varnostnih ravni in podpira uporabnike pri določitvi varnostnih zahtev in izbiri ustreznega ponudnika na podlagi varnostnih zahtev projekta.

Čeprav so informacije o mehanizmih varnosti in zasebnosti pogosto spregledane, bi morali vsi ponudniki storitev v oblaku zagotoviti celovit pregled ravni varnosti, ki jih izpolnjujejo njihove storitve. To bi uporabnikom omogočilo sprejemanje informiranih odločitev na podlagi njihovih varnostnih zahtev.

Na splošno naše ugotovitve poudarjajo potrebo po izboljšanju varnostnih praks med ponudniki storitev v oblaku. Ponudniki morajo povečati preglednost svojih varnostnih mehanizmov in upoštevati ustrezne standarde. Hkrati morajo uporabniki povečati svojo ozaveščenost o varnostnih tveganjih, povezanih z okolji CDE, ter izbrati ponudnika, ki izpolnjuje njihove zahteve glede varnosti in zasebnosti.

8 ZAHVALA

Raziskavo je podprla Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije v okviru financiranja mladih raziskovalcev in raziskovalnega programa E-Gradbeništvo (P2-0210).

9 LITERATURA

Autodesk, informativni dokument o varnosti - https://www.autodesk.com/bim-360/construction-management-software/security, Autodesk Construction Cloud, 2022.

Bamasoud, D. M., Al-Dossary, A. S., Al-Harthy, N. M., Al-Shomrany, R. A., Alghamdi, G. S., Algahmdi, R. O., Privacy and Security Issues in Cloud Computing: A Survey Paper, 2021 International Conference on Information Technology (ICIT), 387–392, https://doi.org/10.1109/ICIT52682.2021.9491632, 2021.

BSI, ISO 19650 Building Information Modelling (BIM), https://www.bsigroup.com/en-ID/bim-building-information-modelling-iso-19650, The British Standards Institution, 2023.

Cerić, A., Vukomanović, M., Ivić, I., Kolarić, S., Trust in megaprojects: A comprehensive literature review of research trends, International Journal of Project Management, 39(4), 325–338, https://doi.org/10.1016/j.ijproman.2020.10.007, 2021.

CSA, SecaaS Category 10 // navodila za izvajanje varnosti omrežja - https://cloudsecurityalliance.org/artifacts/secaas-category-10-network-security-implementation-guidance/, Cloud Security Alliance, 2012.

CSA, varnostne smernice za računalništvo v oblaku - https://cloudsecurityalliance.org/research/guidance/, Cloud Security Alliance, 2021.

Dalux, pogodba o obdelavi podatkov - https://www.dalux.com/wp-content/uploads/2022/08/Data-Processing-Agreement_en-2.pdf, 2020.

Dalux, obvestilo o zasebnosti - https://www.dalux.com/privacy-policy, Dalux, 2023a.

Dalux, pogoji in določila za nekomercialno uporabo Daluxovih storitev - https://www.dalux.com/terms-and-conditions-non-commercial-use, Dalux, 2023b.

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., Bashir, M. N., Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?, 2017 IEEE

10th International Conference on Cloud Computing (CLOUD), 50–57, https://doi.org/10.1109/CLOUD.2017.16, 2017.

GeeksforGeeks, varnostni standardi v oblaku - https://www.geeksforgeeks.org/cloud-security-standards, 2023.

Mahamadu, A.-M., Mahdjoubi, L., Booth, C., Challenges to BIM--Cloud Integration: Implication of Security Issues on Secure Collaboration, 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 209–214, https://doi.org/10.1109/CloudCom.2013.127, 2013.

Manvi, S. S., Shyam, G. K., Cloud Computing: Concepts and Technologies (1st ed.), CRC Press, Taylor & Francis, 2021.

ISO, ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity, 2011.

ISO, ISO/IEC 27001:2013, Information security management systems, International Organization for Standardization, 2013.

ISO, ISO/IEC 27017:2015, Code of practice for information security controls based on ISO/IEC 27002 for cloud services, International Organization for Standardization, 2015.

ISO, ISO/IEC 27000 family, Information security management, International Organization for Standardization, 2018.

ISO, ISO/IEC 27018:2019, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, International Organization for Standardization, 2019.

ISO, ISO 19650-5:2020, Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 5: Security-minded approach to information management, International Organization for Standardization, 2020.

ISO, ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection, Information security management systems, International Organization for Standardization, 2022a.

ISO, ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection, Information security controls, International Organization for Standardization, 2022b.

Pavithra, S., Ramya, S., Prathibha, S., A Survey On Cloud Security Issues And Blockchain, 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), 136–140, https://doi.org/10.1109/ICCCT2.2019.8824891, 2019.

Procore, obvestilo o zasebnosti - https://www.procore.com//legal/privacy, Procore, 2023a.

Procore, standardi varnosti in upravljanja podatkov - https://www.procore.com//trust-and-security/security, Procore, 2023b.

SIST, SIST EN ISO 19650-1:2019, Organizacija in digitalizacija informacij v gradbeništvu - Upravljanje informacij z BIM - 1. del: Pojmi in načela (ISO 19650-1:2018), Slovenski inštitut za standardizacijo, Ljubljana, 2019a.

SIST, SIST EN ISO 19650-2:2019, Organizacija in digitalizacija informacij v gradbeništvu - Upravljanje informacij z BIM - 2. del: Faza načrtovanja in izvedbe gradbenega projekta (ISO 19650-2:2018), Slovenski inštitut za standardizacijo, Ljubljana, 2019b.

SIST, SIST EN ISO 19650-3:2020, Organizacija in digitalizacija informacij v gradbeništvu - Upravljanje informacij z BIM - 3. del: Obratovalna faza sredstev (ISO 19650-3:2020), Slovenski inštitut za standardizacijo, Ljubljana, 2020a.

SIST, SIST EN ISO 19650-5:2020, Organizacija in digitalizacija informacij v gradbeništvu - Upravljanje informacij z BIM - 5. del: Varnostni pristop k upravljanju informacij (ISO 19650-5:2020), Slovenski inštitut za standardizacijo, Ljubljana, 2020b.

SIST, SIST EN ISO 19650-4:2023, Organizacija in digitalizacija informacij v gradbeništvu - Upravljanje informacij z BIM - 4. del: Izmenjava informacij (ISO 19650-4:2022), Slovenski inštitut za standardizacijo, Ljubljana, 2023.

Sun, X., Critical Security Issues in Cloud Computing: A Survey, 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), 216–221, https://doi.org/10.1109/BDS/HPSC/IDS18.2018.00053, 2018.

Trimble, zmogljivosti - https://connect.trimble.com/capabilities, Trimble Connect, 2023a.

Trimble, varstno podatkov in skladnost za gradbeno industrijo - https://www.viewpoint.com/security, Trimble Viewpoint, 2023b.

Xu, H., Cao, J., Zhang, J., Gong, L., Gu, Z., A Survey: Cloud Data Security Based on Blockchain Technology, 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), 618–624, https://doi.org/10.1109/DSC.2019.00100, 2019.