KREPITEV ODPORNOSTI ZA ZAGOTAVLJANJE KIBERNETSKE VARNOSTI V LOKALNIH SKUPNOSTIH

IGOR BERNIK

Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
igor.bernik@um.si

V sodobnem digitalnem okolju se lokalne skupnosti vse pogosteje soočajo z zahtevnimi kibernetskimi izzivi, ki presegajo zgolj tehnično raven in vključujejo kompleksne družbene, organizacijske in varnostne dimenzije. Prispevek izhaja iz koncepta odpornosti (ang. *resilience*) in ga aplicira na področje kibernetske varnosti v lokalnih okoljih. Predstavljeni so ključni elementi, ki vplivajo na zmožnost lokalnih skupnosti, da zaznavajo, preprečujejo, se odzivajo in okrevajo po kibernetskih incidentih. Analizirani so družbeni dejavniki, kot so digitalna vključenost, zaupanje v lokalne ustanove, krizna komunikacija in vloga zaščite. Potrebna je integracija družboslovnih pristopov v oblikovanje lokalnih strategij kibernetske varnosti, zato predstavljamo smernice za oblikovanje (kibernetsko) odpornih in varnih lokalnih okolij.

DOI
https://doi.org/10.18690/um.fvv.4.2025.17

ISBN
978-961-299-068-8

Ključne besede:
kibernetska varnost, odpornost, lokalne skupnosti, digitalna vključenost, zaščita

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.4.2025.17

ISBN
978-961-299-068-8

Keywords:
cybersecurity,
resilience,
local communities,
digital inclusion,
protection

Strengthening Resilience to Ensure Cybersecurity in Local Communities

Igor Bernik
University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
igor.bernik@um.si

In today's digital environment, local communities are increasingly confronted with complex cybersecurity challenges that extend beyond the technical domain and encompass intricate social, organisational, and security dimensions. This paper draws on the concept of resilience and applies it to cybersecurity in local settings. It presents the key elements that influence the ability of local communities to detect, prevent, respond to, and recover from cyber incidents. Social factors such as digital inclusion, trust in local institutions, crisis communication, and the role of civil protection are analysed. Integrating social science approaches into developing local cybersecurity strategies is essential; therefore, this paper offers guidelines for building (cyber) resilient and secure local environments.

University of Maribor Press

1 Uvod

Lokalne skupnosti predstavljajo osnovno raven delovanja družbe, saj prebivalcem zagotavljajo temeljne storitve, od infrastrukture in šolstva do zdravstvene oskrbe. S procesom digitalizacije postajajo v celoti odvisne od informacijskih in komunikacijskih tehnologij, kar pa jih izpostavlja kibernetskim tveganjem. Napadi na občinske sisteme lahko ohromijo delovanje kritičnih storitev, znižajo zaupanje prebivalcev in povzročijo dolgoročne gospodarske ter socialne posledice (Hossain, 2025). Čeprav se kibernetska varnost pogosto obravnava kot tehnično vprašanje, se v zadnjih letih krepi koncept odpornosti (ang. *resilience*), ki združuje tehnične, organizacijske, družbene in institucionalne vidike (de Araujo idr., 2024; Dunn Cavelty idr., 2023). Namen prispevka je tako prikazati ključne elemente krepitve odpornosti lokalnih skupnosti na kibernetske grožnje ter oblikovati priporočila za slovenski kontekst.

2 Koncept odpornosti in kibernetska varnost

Koncept odpornosti izhaja z različnih znanstvenih področij, od ekologije do psihologije, v kibernetskem prostoru pa pomeni zmožnost sistema, da zazna grožnje, se nanje odzove, omeji posledice in se iz njih uči. Ključno je razumevanje, da odpornost ni statična lastnost, temveč proces stalnega prilagajanja. Tehnični elementi, kot so sistemi zaznave in odzivanja, so nujni, a niso dovolj. Raziskave poudarjajo, da ima družbeni kapital – zaupanje v ustanove, pripravljenost na sodelovanje in digitalna pismenost – enako pomembno vlogo pri krepitvi odpornosti (Joinson idr., 2023). Za lokalne skupnosti to pomeni, da morajo vlagati v znanje prebivalcev, graditi povezave z nacionalnimi ustanovami in razvijati načrte neprekinjenega delovanja.

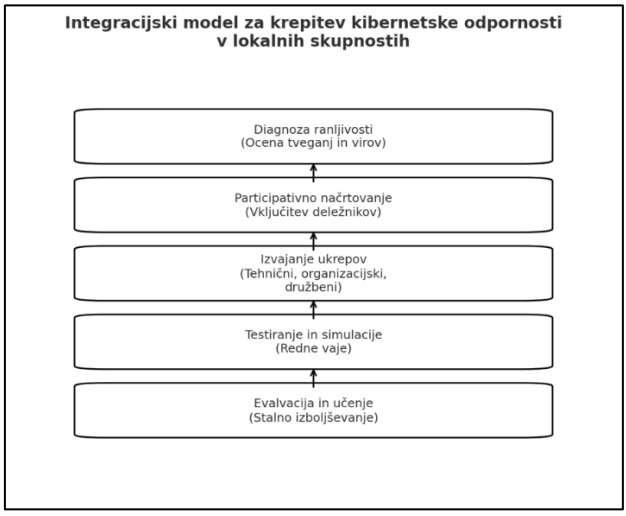
Slovenija se je v zadnjih letih vključila v evropske pobude za krepitev kibernetske varnosti, zlasti z implementacijo direktive NIS2 – *Network and Information Security_2* (European Commission, 2025). Novi Zakon o informacijski varnosti (»Zakon o informacijski varnosti (ZInfV-1)«, 2025) določa obveznosti za javne subjekte, Urad vlade Republike Slovenije za informacijsko varnost pa pripravlja priročnike in koordinira nacionalni odziv (Boštjančič Putko idr., 2025). Operativno raven zagotavljata SI-CERT in SIGOV-CERT, ki delujeta kot odzivni skupini za incidente. Na lokalni ravni delujejo programi ozaveščanja, kot sta Safe.si in Varni na internetu, ki prebivalcem in šolam nudita izobraževanja in gradiva (Safe.si, n. d.; Varni na

internetu, n. d.). Fakulteta za varnostne vede Univerze v Mariboru aktivno razvija strategije izboljšanja digitalne varnosti skozi raziskovalne projekte in Kompetenčni center za kibernetsko in informacijsko varnost (Univerza v Mariboru, Fakulteta za varnostne vede, n. d. a.), pri čemer redno prenaša najsodobnejše znanje na različne udeležence, kot so mestna redarstva, šolniki in strokovnjaki za upravljanje tveganj. Kljub temu ostajajo izzivi: omejena sredstva občin, pomanjkanje strokovnjakov ter nizka digitalna pismenost v posameznih skupinah prebivalstva.

3 Model kibernetske odpornosti lokalnih skupnosti

V lokalnih skupnostih je zato ključno razviti model, ki povezuje omenjene štiri ravni:

- Tehnično raven, ki vključuje orodja za zaznavanje, odzivanje in varnostne politike.
- Organizacijsko raven, ki zajema načrte neprekinjenega delovanja, redne vaje ter jasno določene odgovornosti.
- Družbeno raven, ki temelji na ozaveščanju prebivalcev, spodbujanju digitalne pismenosti in vključevanju ranljivih skupin.
- Institucionalno raven, ki zajema sodelovanje z državnimi organi in certifikacijskimi telesi.



Slika 1: Integracijski model za krepitev kibernetske odpornosti v lokalnih skupnostih.
Vir: lasten.

Ti štirje stebri se povezujejo v ciklični proces petih korakov: diagnoza ranljivosti, načrtovanje, izvedba ukrepov, testiranje ter evalvacija in učenje (Tzavara in Vassiliadis, 2024).

S takšnim modelom lahko lokalne skupnosti dolgoročno gradijo odpornost. Integracijski model (Slika 1) je adaptiven in cikličen, kar pomeni, da ga je treba stalno ponavljati in nadgrajevati. Poudarek ni na popolni zaščiti, temveč na zmožnosti preživetja, hitrem okrevanju in učenju.

4 Primeri in možnosti za Slovenijo

Iz tujine poznamo več uspešnih praks. V ZDA so po odmevnih incidentih mest, kot sta Baltimore in New Orleans, uvedli krizne centre in partnerstva z zasebnimi podjetji (Associated Press, 2025; National League of Cities, n. d.). V Evropski uniji so projekti, ki spodbujajo povezovanje mest, podjetij in prebivalcev, prepoznani kot učinkovit okvir (European Union Agency for Cybersecurity [ENISA], n. d.). V Skandinaviji občine sodelujejo v skupnih centrih za odpornost, kar omogoča delitev znanja in stroškov (OECD, n. d.). Jarjoui idr. (2024) je predstavil koncept *community-centered cyber resilience*, ki prebivalce vključuje kot aktivne akterje v procesih zaščite. Na podlagi teh primerov je mogoče oblikovati predlog za Slovenijo: medobčinski center za kibernetsko odpornost, ki bi združeval tehnične kapacitete, skupne vaje in programe ozaveščanja. Takšen center bi manjšim občinam omogočil dostop do znanja in virov, ki jih same ne zmorejo vzpostaviti.

5 Tveganja in omejitve

Vzpostavitev modelov varnosti ni brez izzivov. Finančne omejitve občin pomenijo, da je nujna državna ali evropska podpora. Kadrovska vrzel, zlasti pomanjkanje strokovnjakov, se lahko nadomesti s partnerstvi z univerzami in skupnimi strokovnimi ekipami. Organizacijska tveganja vključujejo nejasno razmejitev odgovornosti, ki jo je mogoče reševati s formaliziranimi protokoli. Socialna tveganja se kažejo v nizki digitalni pismenosti prebivalcev, zato so potrebne stalne delavnice in kampanje. Politična tveganja izhajajo iz odpora do centralizacije, kar je mogoče nasloviti z modeli, ki ohranjajo avtonomijo občin, ob hkratnem deljenju virov (OECD, n. d.).

6 Diskusija in zaključki

Kibernetska odpornost na lokalni ravni je kompleksen proces, ki presega tehnično zaščito. Poudariti je treba, da odpornost ni končno stanje, temveč proces stalnega prilagajanja in učenja (Groenendaal in Helsloot, 2021). Ključni izzivi so stroški, kadrovski primanjkljaj in pomanjkanje sodelovanja med občinami, a izkušnje iz tujine dokazujejo, da so skupni centri in mreže izvedljivi. Interdisciplinarni pristop, ki povezuje tehniko, družboslovje in politiko, je nujen za trajnostne rešitve (Dunn Cavelty idr., 2023). Akademske ustanove imajo pri tem ključno vlogo, saj premoščajo vrzel med teorijo in prakso ter zagotavljajo kapacitete za občine, ki same ne zmorejo razviti obsežnih rešitev. V prihodnje je potrebno več vlaganj v partnerstva občin, podporne državne mehanizme in raziskave, ki bodo povezale lokalne potrebe z globalnimi trendi kibernetske odpornosti. Potrebno je povezovanje informatikov, sociologov, psihologov, pravnikov, strokovnjakov za krizno komuniciranje in menedžmenta. Le tako lahko zagotovimo, da tehnične rešitve podpirajo tudi organizacijske in družbene spremembe, ki so potrebne za učinkovito odpornost.

V omenjenem kontekstu je posebej pomembna tudi vloga akademskih ustanov. Fakulteta za varnostne vede Univerze v Mariboru z raziskovalnimi projekti, kot je npr. projekt SCREEN (Univerza v Mariboru, Fakulteta za varnostne vede, n. d. b.) in v okviru Kompetenčnega centra za kibernetsko in informacijsko varnost (Univerza v Mariboru, Fakulteta za varnostne vede, n. d. a.) neposredno prispeva k razvoju strategij izboljšanja digitalne varnosti in odpornosti. Sodelovanje z lokalnimi akterji – od predavanj mestnemu redarstvu v Ljubljani, delavnic za učitelje osnovnih in srednjih šol do usposabljanj za profesionalce s področja obvladovanja tveganj – predstavlja način, kako se najsodobnejše znanje (hitro) prenaša v prakso. Vloga akademskih ustanov je tako ključna pri premostitvi vrzeli med teorijo in prakso ter pri zagotavljanju kapacitet za občine, ki same ne morejo razviti obsežnih rešitev. Akademske ustanove delujejo kot most med raziskovalnimi spoznanji in konkretnimi potrebami lokalnega okolja.

Če strnemo, je pot do kibernetsko odpornih lokalnih skupnosti v Sloveniji utemeljena na kombinaciji tehničnih, organizacijskih, družbenih in institucionalnih elementov, ki jih povezuje stalni proces učenja in prilagajanja. Akademske ustanove imajo pri tem posebno vlogo kot posredniki znanja, inovacij in podpore, brez katerih lokalne skupnosti težko samostojno razvijejo trajnostne rešitve. S predlaganim

povezovanjem je mogoče zagotoviti, da bodo slovenske občine v digitalni družbi prihodnosti oziroma Družbi 5.0 varne, odporne in zaupanja vredne.

Viri in literatura

Associated Press. (27. 5. 2025). *Iranian pleads guilty to ransomware attacks that affected Baltimore, other cities.* https://apnews.com/article/ransomware-plea-federal-court-iran-cities-aab689b79d5c9eb4ea78c9a77a997ffd

de Araujo, M. S., Machado, B. A. S. in Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. *Applied Sciences, 14*(5), 2116. doi:10.3390/app14052116

Dunn Cavelty, M., Eriksen, C. in Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research, 26*(7), 801–814. doi:10.1080/13669877.2023.2208146

Boštjančič Putko, I., Božič, G., Čaleta, D., Čaleta, M., Jakopin, B., Jerina, P., Mravljak, M. in Obreht, M. (2025). *Priročnik kibernetske varnosti. Urad Republike Slovenije za informacijsko varnost.* https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf

European Commission. (2025). *NIS2 Directive: securing network and information systems.* https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Union Agency for Cybersecurity (ENISA). (n. d.). *Topics.* https://www.enisa.europa.eu/?utm_source=chatgpt.com#contentList

Groenendaal, J. in Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. *Journal of Contingencies and Crisis Management, 29*(4), 439–444. doi:10.1111/1468-5973.12360

Hossain, S. T., Yigitcanlar, T., Nguyen, K. in Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework key challenges. *Urban Governance, 5*(1), 1–19. doi:10.1016/j.ugj.2024.12.010

Jarjoui, S. Murimi, R. in Murimi, R. (2024). Communities, agency, and resilience: A perspective addressing tragedy of the cyber commons. *The Cyber Defense Review, 9*(1), 113–131.

Joinson, A. N., Dixon, M., Coventry, L. in Briggs, P. (2023). Development of a new 'human cyber-resilience scale'. *Journal of Cybersecurity, 9*(1). doi:10.1093/cybsec/tyad007

National League of Cities. (n. d.). *News & insights.* https://www.nlc.org

OECD. (n. d.). *Topics.* https://www.oecd.org/

Safe.si. (n. d.). *Umetna inteligenca.* https://safe.si

Tzavara, V. in Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security, 23,* 1695–1719. doi:10.1007/s10207-023-00811-x

Univerza v Mariboru, Fakulteta za varnostne vede. (n. d. a.). *Kompetenčni center za kibernetsko in informacijsko varnost.* https://www.fvv.um.si/vstopna-stran/o-fakulteti/organiziranost/kompetencni-center-za-kibernetsko-in-informacijsko-varnost/

Univerza v Mariboru, Fakulteta za varnostne vede. (n. d. b.).. *Premostitev digitalnega razkoraka – okvir kompetenc za kibernetsko varnost za starejše odrasle (projekt SCREEN, J5-60085).* https://www.fvv.um.si/vstopna-stran/raziskovalna-dejavnost/temeljni-in-ciljni-raziskovalni-projekti/premostitev-digitalnega-razkoraka-okvir-kompetenc-za-kibernetsko-varnost-za-starejse-odrasle/

Varni na internetu. (n. d.). *Najpogostejše težave, s katerimi se soočajo spletni uporabiki.* https://www.varninainternetu.si/?utm_source=chatgpt.com

Zakon o informacijski varnost (ZInfV-1). (2025). *Uradni list RS,* (40/25).