IZVJEŠTAJ

STANJE DIGITALNE BEZBJEDNOSTI U CRNOGORSKIM MEDIJIMA

MEDIJSKA ASOCIJACIJA JUGOISTOČNE EVROPE

AUTOR: VUK MARAS

MASE

Reporting Digital Rights & Freedoms

Funded by the European Union

IZVJEŠTAJ

STANJE DIGITALNE BEZBJEDNOSTI U CRNOGORSKIM MEDIJIMA

Autor: Vuk Maras

Oktobar 2025. godine

O autoru

Vuk Maraš ima preko 20 godina iskustva u radu sa medijima u Crnoj Gori i regionu. Bio je programski direktor MANS-a baveći se monitoringom i analitikom sprovođenja zakona i funkcionisanja institucija, a nakon toga obavljao je funkciju izvršnog direktora MASE. Od 2023. godine nalazi se na funkciji izvršnog direktora BIRN Crna Gora.

Učestvovao je u izradi seta medijskih zakona u Crnoj Gori kao i prve Medijske strategije. Autor je brojnih analiza i izvještaja za različite organizacije u Crnoj Gori, regionu i šire.

Izdavač: Medijska Asocijacija Jugoistočne Evrope
Trg Nezavisnosti BB, 81000 Podgorica
www.masee.org

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of MASE and do not necessarily reflect the views of the EU.

MASE

Reporting Digital Rights & Freedoms

Funded by the European Union

UVOD

Digitalna bezbjednost postaje jedno od najvažnijih pitanja za rad medija u Crnoj Gori. Novinari i redakcije sve češće se suočavaju s pokušajima kompromitacije, digitalnim napadima i rizicima po bezbjednost podataka. Iako tehnološki razvoj omogućava bržu i efikasniju komunikaciju, istovremeno otvara prostor za nove vrste prijetnji – od DDoS napada i phishing poruka do pokušaja nadzora i lažnog predstavljanja.

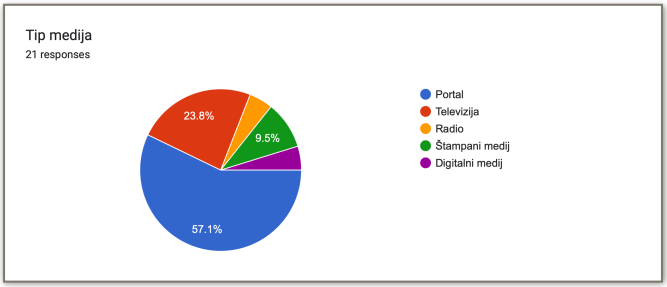
Medijska asocijacija Jugoistočne Evrope (MASE) sprovela je tokom oktobra 2025. godine anketu među crnogorskim medijima s ciljem da se sagleda stvarno stanje digitalne bezbjednosti, postojeći kapaciteti i praksa reagovanja u slučaju napada. Anketom je obuhvaćeno 21 medij različitog profila, uključujući portale, televizije, radio i štampane medije.

Kako su mediji izrazili želju da anketa bude anonimna, upravo zbog zaštite od potencijalnih napada, njihova imena nisu navedena u izvještaju.

SADRŽAJ

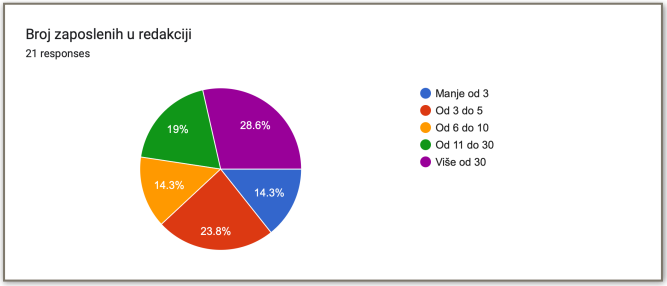
1.
PROFIL UČESNIKA

Od ukupno 21 medija koji su učestvovali u istraživanju, najviše ih je portala, ukupno 12, zatim pet televizija, dva štampana medija, te po jedan radio i digitalni medij.



Grafik 1: Profil medija

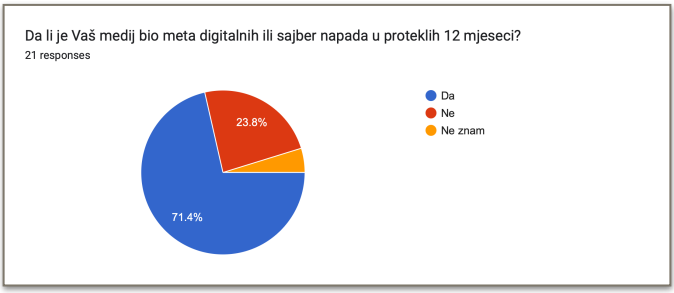
Broj zaposlenih u redakcijama kreće se od manjih timova s troje do petoro ljudi, do redakcija koje imaju više od 30 zaposlenih. Ovakva struktura omogućava uvid u stanje kako kod malih lokalnih, tako i kod većih nacionalnih medija ili javnih emitera.



Grafik 2: Broj zaposlenih u medijima

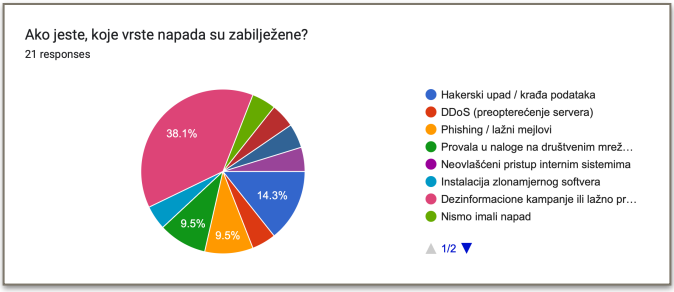
2.
UČESTALOST Nnapada

Čak 15 od 21 medija (71%) izjavilo je da su u proteklih godinu dana bili meta digitalnog ili sajber napada. Pet redakcija (24%) navelo je da nijesu bile napadnute, dok je jedan ispitanik odgovorio da nije siguran da li je bilo napada.



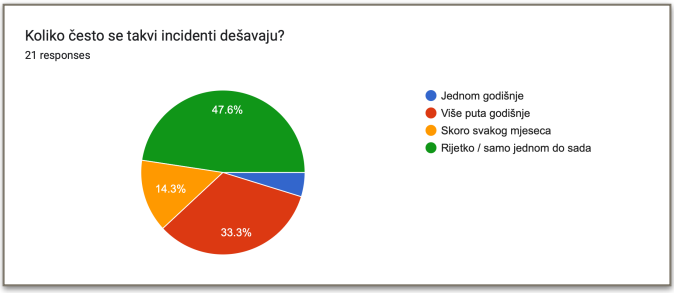
Grafik 3: Dešavanje napada

Najčešće prijavljeni napadi uključuju DDoS napade i phishing poruke, zatim dezinformacione kampanje, pokušaje instalacije zlonamjernog softvera, kao i lažno predstavljanje putem mejlova ili društvenih mreža. U nekoliko slučajeva mediji su prijavili pokušaje nadzora komunikacije ili krađe korisničkih podataka.



Grafik 4: Vrste napada

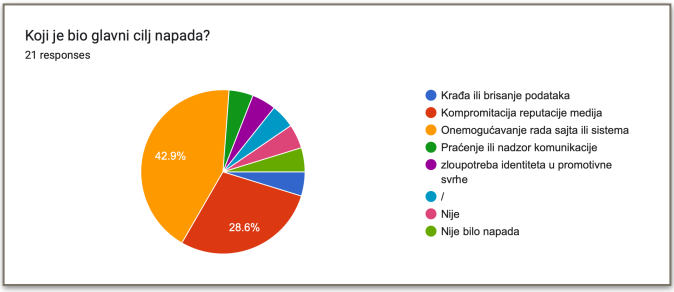
Po učestalosti, većina ispitanika navodi da se incidenti dešavaju povremeno – "rijetko" ili "jednom godišnje". Međutim, tri medija su prijavila da se napadi događaju gotovo svakog mjeseca, što ukazuje na kontinuiranu izloženost i visok nivo rizika.



Grafik 5: Učestalost napada

3.
CILJEVI NAPADA

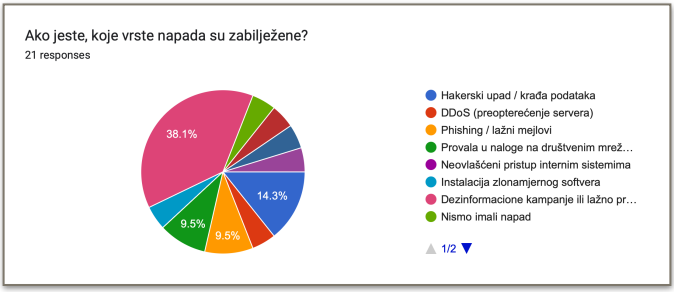
Najčešće prepoznati ciljevi napada su:
- onemogućavanje rada sajta ili sistema (43%),
- kompromitacija reputacije medija (33%),
- i praćenje komunikacije (10%).



Grafik 6: Ciljevi napada

Ovi podaci ukazuju da sajber napadi na medije nijesu slučajni, već imaju jasan cilj – utišavanje ili otežavanje rada redakcija, posebno onih koje objavljuju osjetljive sadržaje.

Same redakcije prepoznaju najviše dezinformacione kampanje ili lažno predstavljanje kao jedan od najčešćih vrsta napada (38%), hakerski upad ili krađu podataka (14%), te provala u naloge na društvenim mrežama i phishing i lažni mejlovi sa po 9,5%.



Grafik 7: Vrste napada

Uprkos velikom broju napada, većina medija (oko 70%) nije ih prijavila nadležnim institucijama. Najčešći razlozi za neprijavljivanje su nepovjerenje u institucije, nedostatak informacija kome se obratiti, kao i nedostatak dokaza.

Grafik 8: Prijavljivanje napada

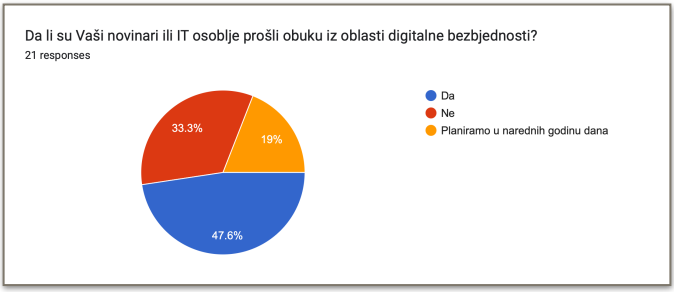
Samo manji broj ispitanika je naveo da su pokušali da kontaktiraju državne organe ili stručnjake, ali bez jasnog odgovora ili povratne informacije. Ovaj rezultat ukazuje na izražen raskorak između medijskog sektora i institucionalnog sistema zaštite u oblasti sajber bezbjednosti.

4.
KAPACITETI

Na pitanje da li imaju uspostavljene interne procedure za sajber bezbjednost, odgovori su gotovo ravnomjerno raspoređeni:
- 7 medija (33%) ima razvijene interne procedure,
- 7 medija (33%) ih nema,
- a 7 medija (33%) ih sprovodi djelimično.

Ovi podaci pokazuju da iako postoji određena svijest o značaju digitalne bezbjednosti, formalizovani sistemi zaštite u redakcijama još uvijek nijesu standardna praksa.

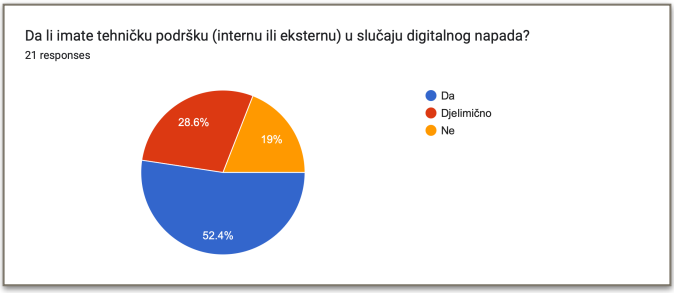
Skoro polovina ispitanih medija (10 od 21) navela je da su njihovi novinari ili IT osoblje prošli neku vrstu obuke iz oblasti digitalne bezbjednosti. Još četiri medija planiraju da obuke sprovedu u narednih godinu dana, dok ih sedam (33%) nema takvih planova.



Grafik 9: Obučenost osoblja

Ovaj rezultat pokazuje da, iako raste interesovanje za edukaciju u ovoj oblasti, znatan broj redakcija i dalje nema osnovna znanja o zaštiti podataka, bezbjednom korišćenju komunikacionih kanala i prepoznavanju digitalnih prijetnji.

Na pitanje o dostupnosti tehničke podrške, 11 medija (52%) navelo je da ima internu ili eksternu podršku u slučaju digitalnog napada, šest (29%) je djelimično pokriveno, dok četiri medija (19%) uopšte nemaju nikakvu tehničku pomoć.



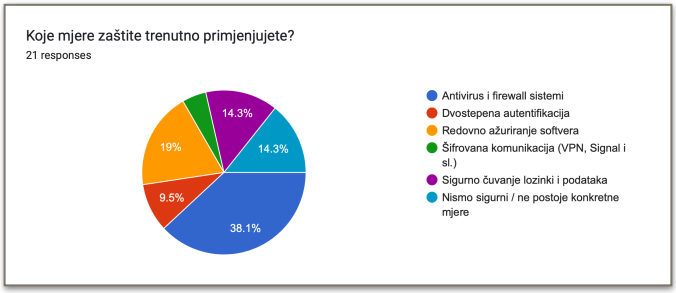
Grafik 9: Dostupnost tehničke podrške

Podaci pokazuju da veće redakcije, koje imaju IT sektor ili eksternog partnera, lakše odgovaraju na digitalne prijetnje, dok manji lokalni mediji ostaju bez podrške u kriznim situacijama.

5.
NIVO DIGITALNE BEZBJEDNOSTI

Prosječna ocjena opšteg nivoa digitalne bezbjednosti medija iznosi 2,9 od 5, što ukazuje na umjeren nivo zaštite. Nijedan medij nije dao najvišu ocjenu, što potvrđuje da postoji svijest o postojećim slabostima.

Najčešće mjere koje redakcije koriste su antivirus i firewall sistemi, sigurno čuvanje lozinki, i u manjoj mjeri dvofaktorska autentifikacija. Ipak, malo redakcija ima uspostavljene politike redovnih bezbjednosnih provjera ili automatizovane sigurnosne kopije podataka.



Grafik 10: Mehanizmi zaštite

6.
KOMENTARI UČESNIKA

U otvorenim odgovorima učesnici su istakli nekoliko zajedničkih izazova:
- potrebu za obukama zaposlenih, posebno za novinare koji nijesu tehnički potkovani;
- nedostatak finansijskih sredstava za zaštitne softvere i tehničku opremu;
- nepostojanje jasnog kanala komunikacije s državnim institucijama;
- rast spam i lažnih poruka koje dolaze s domaćih i stranih servera.

Istraživanje jasno pokazuje da sajber prijetnje postaju sve češće, dok su kapaciteti medija da na njih odgovore i dalje ograničeni. Prosječna ocjena ispod 3, uz činjenicu da dvije trećine medija nema kompletne interne procedure, potvrđuje potrebu za sistemskim pristupom.

Digitalna bezbjednost nije samo tehničko, već i profesionalno pitanje jer direktno utiče na slobodu izražavanja, zaštitu izvora i integritet novinarstva u Crnoj Gori.

7.
ZAKLJUČCI I PREPORUKE

Anketa pokazuje da su mediji u Crnoj Gori svjesni rizika, ali da u praksi raspolažu ograničenim kapacitetima za efikasnu zaštitu. Većina napada ostaje neprijavljena, a tehnička i institucionalna podrška medijima gotovo da ne postoji. S obzirom na porast broja napada i njihovu složenost, neophodno je razviti sistemske mjere koje će ojačati otpornost medijskog sektora.

Preporuke:
1. Razviti nacionalni program za jačanje digitalne otpornosti medija.
2. Obezbijediti kontinuirane obuke i radionice za novinare, urednike i IT osoblje.
3. Uspostaviti jedinstveni institucionalni kanal za prijavljivanje digitalnih napada i intenzivno ga promovisati.
4. Podržati male i lokalne redakcije kroz grantove i tehničku pomoć za unapređenje digitalne bezbjednosti..
5. Uključiti digitalnu bezbjednost u programe medijske pismenosti.
6. Podstaći saradnju među medijima u razmjeni iskustava i zajedničkoj reakciji.
7. Promovisati razvoj internih politika bezbjednosti u medijima.