*Sažetak*

# Procjena kibernetičke sigurnosti i izbora u Bosni i Hercegovini

**Mart 2020**

# *Sažetak*
# Procjena kibernetičke sigurnosti i izbora u Bosni i Hercegovini

Mart 2020


Sažetak: Procjena kibernetičke sigurnosti i izbora u Bosni i Hercegovini


International Foundation for Electoral Systems
2011 Crystal Drive, 10th Floor
Arlington, VA 22202
Email: editor@ifes.org
Fax: 202.350.6701

*This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of USAID or the United States Government.*

# Procjena kibernetičke sigurnosti i izbora u Bosni i Hercegovini

## Sažetak

Tijela za provođenje izbora diljem svijeta našla su se na udaru žestokih napada usmjerenih na podrivanje legitimiteta izbornog procesa. Premda su brojna tijela izgradila odbrambene mehanizme, obim i sofisticiranost napada na demokratske sisteme i institucije i dalje se intenzivira na regionalnom i globalnom nivou. Iako nijedan otkriveni napad još uvijek nije uticao na izborne procese u Bosni i Hercegovini (BiH), neophodno je da se Centralna izborna komisija (CIK) pripremi kako za oportunističke napade koji za cilj imaju ostvarivanje finansijske dobiti, poput ucjenjivačkih (ransomware) napada koji se izvode protiv organizacija lokalne i centralne vlasti širom svijeta, tako i politički motivisanih napada usmjerenih protiv izbornog sistema u cjelini.

Međunarodna fondacija za izborne sisteme (IFES) izrađuje strategije za tijela za provođenje izbora s ciljem jačanja njihovih tehnologija i procedura za otklanjanje uočenih ranjivosti u skladu sa vlastitim procesom Sveobuhvatnog ispitivanja izloženosti i prilagođavanja - *Holistic Exposure and Adaptation Testing (HEAT).* Budući da niti jedan izborni proces ili tehnologija nisu nepogrješivi , proces HEAT nastoji prepoznati i ispitati moguće zloupotrebe postojećih ranjivosti tehnologije za upravljanje izborima i pravnih i operativnih okvira unutar kojih ta tehnologija djeluje. Ovom se metodologijom vrši procjena tehnološke, kadrovske, političke, pravne i proceduralne izloženosti i podstiče sveobuhvatna analiza svih oblasti u kojima bi se problemi mogli pojaviti.

Priprema Procjene kibernetičke sigurnosti i izbora (u daljem tekstu „Procjena“) podrazumijevala je analizu nalaza iz prethodnih izvještaja IFES-a, javno dostupnih informacija sa interneta i održavanje niza sastanaka i konsultacija sa relevantnim akterima, čiji je spisak dat u prilogu ovog izvještaja, a koji su održani između 9.3. i 13.3. ove godine. Procjenu je predvodio tim za kibernetičku sigurnost i izbore IFES-a u kojem su bili savjetnik za tehnologiju i kibernetičku sigurnost IFES-a i vođa tima Thomas Chanussot, ekspert za kibernetičku sigurnost informacionu sigurnost Srđan Babić, regionalna direktorica IFES-a za Evropu i Evroaziju dr. Beata Martin-Rozumiłowicz i ekspert IFES-a za izbornu tehničku pomoć Nermin Nišić. Analiza dokumentacije i održane konsultacije pružile su članovima tima potrebne informacije o izazovima sa kojima se CIK suočava, trenutnom stanju vezanom za kibernetičku sigurnost u BiH, resursima koji se odnose na kibernetičku sigurnost, te prijetnje sa kojima se suočava BiH.

Tim je utvrdio da su kapaciteti i zakonodavni okvir koji se odnose na kibernetičku sigurnost u BiH još uvijek u ranoj fazi razvoja. Ono što posebno zabrinjava je nepostojanje nacionalnog tijela za koordinaciju i rukovođenje odgovorima na incidente čime je CIK ostavljen bez podrške nadležnih agencija kada je riječ o incidentima koji se odnose na kibernetičku sigurnost.

Ključno osoblje Odsjeka za informaciono-komunikacione tehnologije CIK-a su dugogodišnji zaposlenici koji posjeduju iscrpno operativno razumijevanje izbora, ali im nedostaju tehnički kapaciteti za pružanje kontinuirane podrške postojećim sistemima CIK-a. Potrebno je također navesti da se Odsjek za informaciono-komunikacijske tehnologije suočava sa kritičnim nedostatkom osoblja i resursa; problem zapošljavanja stručnjaka za informaciono-komunikacione tehnologije u javnom sektoru predstavlja globalni problem, naročito u regiji Balkana, i ne odnosi se samo na CIK. Ovo je

dijelom posljedica razlike u visini plata u javnom i privatnom sektoru, što dovodi do nedostatka kvalificiranog osoblja, neadekvatne raspodjele zaduženja zaposlenih čime se stvara rizik od zloupotreba, curenja i neovlaštenog pristupa. CIK je zbog toga ranjiv na interne napade, manipulacije ili sabotaže koje mogu biti finansijski ili politički motivisane.

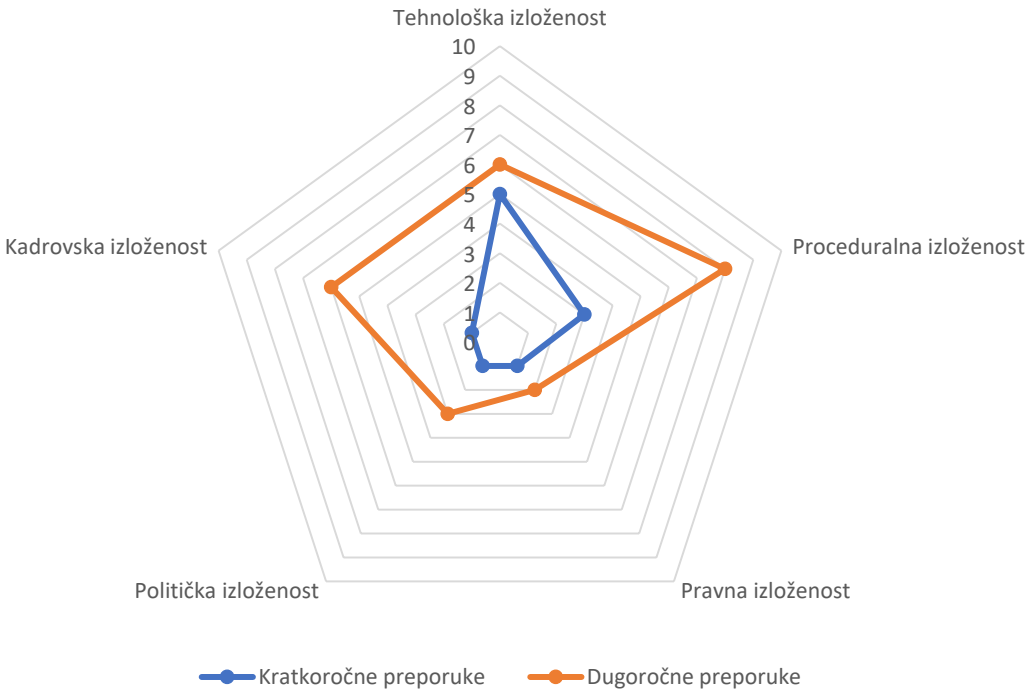
Odsjek za informaciono-komunikacione tehnologije uspio je stvoriti i održati povjerenje među svojim korisnicima; incidenti koji se odnose na kibernetički sigurnost brzo su prijavljivani prije nego li bi eskalirali i negativno uticali na rad. Odsjek za informaciono-komunikacione tehnologije sada treba nastojati da održi ovo povjerenje budući da će i dalje predstavljati prvu liniju odbrane protiv zlonamjernih aktivnosti usmjerenih protiv CIK-a.

Nadalje, CIK nije pripremljen za djelovanje protiv kibernetičkih napada, kako na tehničkom tako i na organizacionom nivou. Servisi dostupni putem weba nemaju odgovarajuću zaštitu i mogu biti kompromitovani umjereno sofisticiranim napadima čime bi integritet podataka i ugled CIK-a bio narušen. Ukupno gledano, CIK nema adekvatnu zaštitu mreže i servise kibernetičke sigurnosti koji bi zaštitili infrastrukturu Komisije. Glavni data centar CIK-a fizički se nalazi u glavnom uredu CIK-a, ali ne postoji back-up centar. Također ne postoji plan oporavka od katastrofa (disaster recovery plan) niti plan kontinuiteta poslovanja čime bi se ublažio rizik tokom krize.

Generalno, CIK-u i većini drugih agencija nedostaje obuka po pitanju kibernetičke sigurnosti kao i resursi za pružanje obuke, što predstavlja glavni nedostatak kada je riječ o odnosu prema kibernetičkoj sigurnosti. Više opštih kurseva na temu podizanja svijesti i znanja o kibernetičkoj sigurnosti bilo bi od koristi za osoblje CIK-a i opštinskih izbornih komisija (OIK) koji nisu stručnjaci za informaciono-komunikacione tehnologije. Osoblju treba pružiti obuku vezano za ranjivosti i prijetnje u smislu kibernetičke sigurnosti te ih osposobiti kako da se nose sa kibernetičkim napadima.

Što se određena organizacija više oslanja na tehnologiju, to je izraženija potreba za pristupom problemu sigurnosti od vrha prema dole. Iako CIK ne primjenjuje glasanje putem interneta ili elektronsko glasanje, ipak je ranjiv u odnosu na brojne interne i vanjske prijetnje. CIK-u je potrebna aktivnost iniciran od strane rukovodstva na osmišljavanju planova za umanjenje rizika koja bi uključivala predstavnike svih odsjeka, a ne samo Odsjeka za informaciono-komunikacione tehnologije.

IFES je u integralnom izvještaju predstavio kratkoročne i dugoročne preporuke za jačanje kapaciteta osoblja, davanje prioriteta jačanju odbrane mreže i infrastrukture i smanjenje ili ublažavanje rizika koji se odnose na kibernetičku sigurnost. Radar dijagram ispod prikazuje vrste preporuka u odnosu izloženost rizicima.




*Slika: Ovaj radar dijagram prikazuje predviđeni efekat preporuka IFES-a u odnosu na rizike kojima je CIK izložen. Dugoročne preporuke se šire prema vani i i pokrivaju veći dio od pet izloženosti navedenih u HEAT procesu. (IFES, 2020).*


Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive | 10th Floor | Arlington, VA 22202 | www.IFES.org