

# Kibernetička sigurnost u malim i srednjim poduzećima: kako napraviti više s ograničenim resursima?

Luka Matić · 15. rujna 2026.

# O meni

01 humanistička pozadina

---

02 iz privacyja u cybersecurity

---

03 iskustvo iz digitalnih transformacija

---

04 R&D u cybersecurityju: FER i CyberArrange

# O čemu pričamo kad pričamo o sigurnosti MSP-a

- 01 zaštita jednostavnih IT sistema
- 02 zaštita tajnosti i integriteta osobnih i povjerljivih podataka
- 03 jednostavna systemska i dubinska zaštita: lozinke, MFA, backup, svijest o prijetnji

# Što se stvarno događa

Napadi su oportunistički, ne ciljani: ukradene lozinke i nezakrpani uređaji, ne industrija ni prihod.

# 96 %

žrtava ransomwarea su mala i srednja poduzeća

# 1/3

svih incidenata u Hrvatskoj je phishing

## BEC U PRAKSI

Dopis na memorandumu stvarnog partnera, potpis, pečat i novi IBAN.

**Šteta: nekoliko stotina tisuća eura.**

# S kojim izazovima se suočavamo? Skepsa

*„Platili smo GDPR usklađivanje pa nam ničemu nije služilo. Zašto bi ovo bilo drugačije?”*

*„Ma neće nas.”*

*„Koliko to košta? To je sigurno skupo.”*

*„Nemam se vremena time baviti, moram voditi firmu.”*

# S kojim izazovima se suočavamo II? Overkill i krivi trošak

## Pretjerivanje

---

- 01 vrlo stroge mjere
- 02 pretjerana produkcija protokola i politika
- 03 hoarding alata

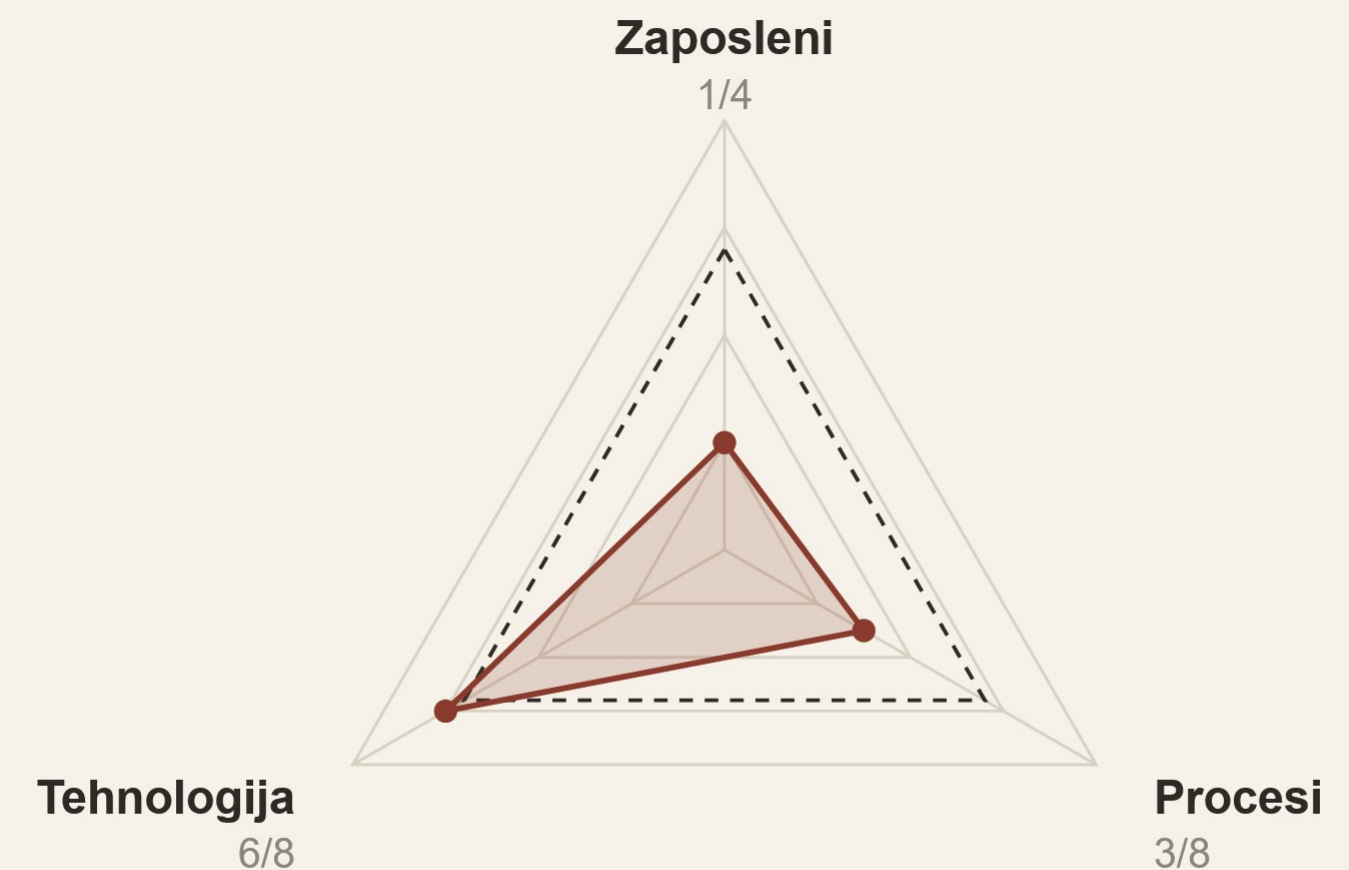
## Krivi trošak

---

- 04 novac odlazi na licence i antivirusne programe, a tehničke mjere su manje učinkovite od ulaganja u ljude
- 05 interni IT koji istovremeno održava sustav i „brine“ o njegovoj sigurnosti: sukob interesa bez svijesti o njemu
- 06 vanjski IT pružatelji često bez sigurnosne svijesti, pa dobivamo ranjive sustave

# Kako zaobići izazove

- 01 jednostavna procjena rizika: samoprocjena u deset pitanja, tri domene, četiri razine zrelosti
- 02 kibernetička sigurnost kao jednostavni sistem
- 03 kibernetička sigurnost kao dubinski sistem
- 04 integracija u svakodnevni rad
- 05 longitudinalni pristup



**Ukupno: 10/20 · Operativna razina**

---- prag sljedeće razine (14/20)

Primjer nalaza instrumenta samoprocjene

# Upitnik samoprocjene: deset pitanja

- |                                                                                                                                                          |                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>01</b> Jesu li vaši zaposlenici upoznati s osnovnim prijetnjama poput lažnih e-mailova (phishing), ransomwarea i sumnjivih web stranica?</p> <hr/> | <p><b>06</b> Postoje li pisana pravila o tome kako zaposlenici smiju koristiti poslovne uređaje i sustave?</p> <hr/>                                      |
| <p><b>02</b> Jesu li svi poslovni uređaji (računala, laptopi, mobiteli) zaštićeni lozinkom i antivirusnim programom?</p> <hr/>                           | <p><b>07</b> Imate li plan što napraviti ako izgubite podatke ili doživite cyber napad – tko što radi, koga zovete?</p> <hr/>                             |
| <p><b>03</b> Ažuriraju li se operativni sustavi i programi na vašim uređajima redovito?</p> <hr/>                                                        | <p><b>08</b> Koristite li dvostupanjsku provjeru identiteta (npr. uz lozinku treba i kod na mobitelu) za e-poštu, bankarstvo ili cloud servise?</p> <hr/> |
| <p><b>04</b> Ima li svaki zaposlenik pristup samo onim podacima i sustavima koji su mu potrebni za posao?</p> <hr/>                                      | <p><b>09</b> Je li netko u poduzeću zadužen za kibernetičku sigurnost – makar kao dio svojih zadataka?</p> <hr/>                                          |
| <p><b>05</b> Izrađuju li se sigurnosne kopije poslovnih podataka i čuvaju li se na odvojenom mjestu (vanjski disk, cloud)?</p>                           | <p><b>10</b> Zna li tko izvana ima pristup vašim poslovnim podacima – npr. računovođa, IT servis, softver u cloudu?</p>                                   |

# Što sutra, što prestati

## KAD INCIDENT KRENE

- prvi puca čovjek, u tri od četiri slučaja
- drugi puca restore backupa

### JEDNA STVAR ZA SUTRA

**password manager i MFA**

### JEDNA STVAR ZA PRESTATI

**oslanjanje isključivo na tehničke mjere**

HUP CYBER PRAKTIKUM

---

# Imate li pitanja?

Hvala na pažnji.

luka@lukamatic.pro · lukamatic.pro · [LinkedIn](#)