HGK
HRVATSKA GOSPODARSKA KOMORA

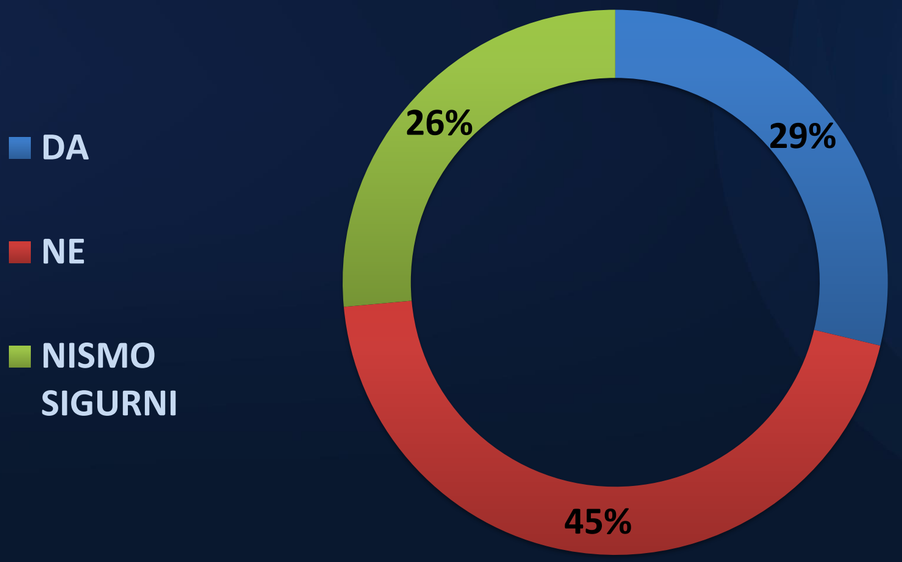
AKADEMIJA KIBERNETIČKE SIGURNOSTI

Uvid u stanje kibernetičke sigurnosti među poduzetnicima u RH 2025, N300

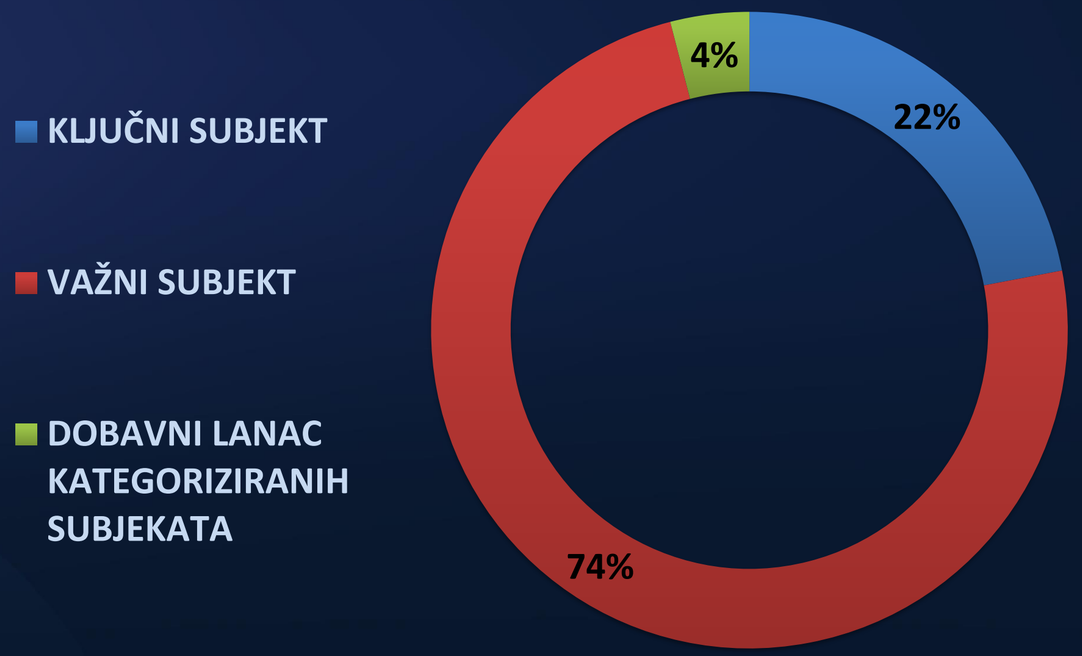
23. prosinca, 2025. Zagreb

1. Je li Vaša organizacija već kategorizirana prema Zakonu o kibernetičkoj sigurnosti RH?

Mnoge organizacije još nisu sigurne pripadaju li pod obveze Zakona, što pokazuje manjak informiranosti i potrebu za jasnijim tumačenjem i komunikacijom regulatornih zahtjeva.

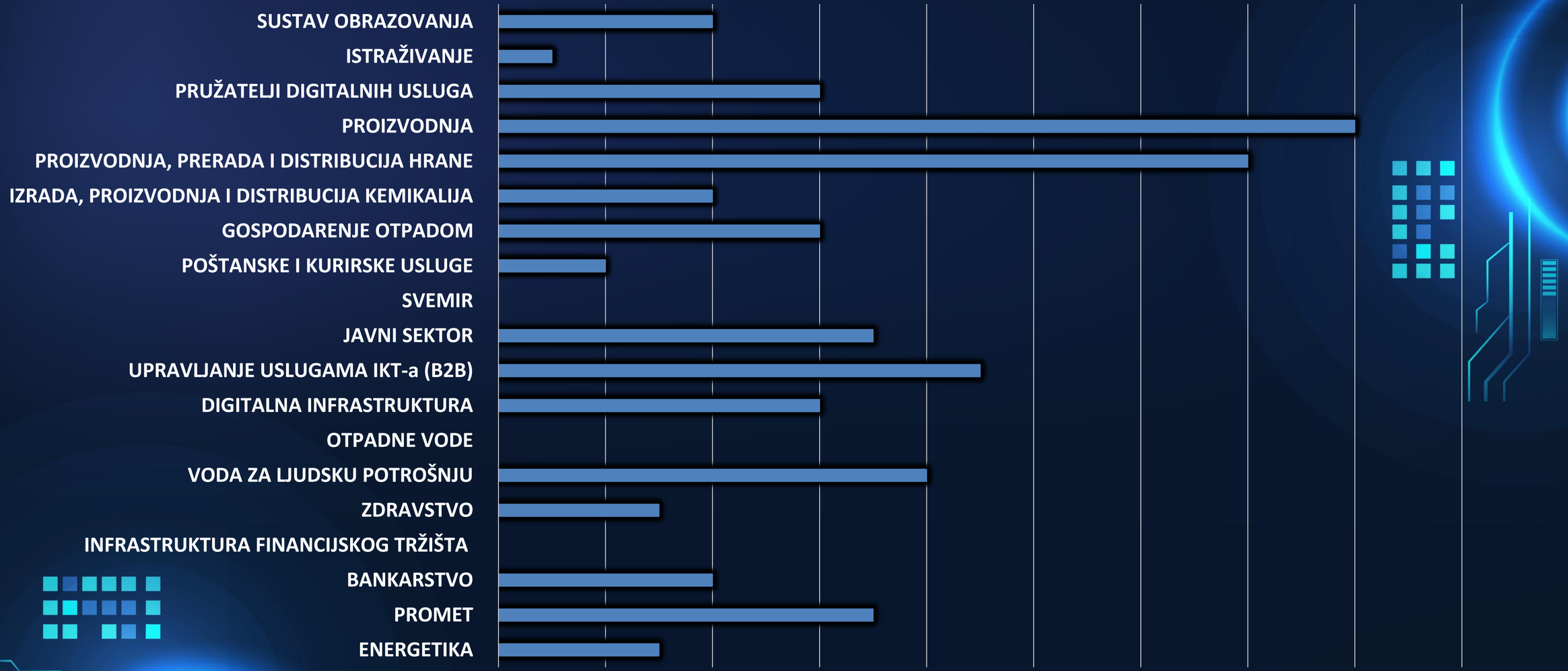


2. Ako je odgovor Da, kako je kategorizirana Vaša organizacija?



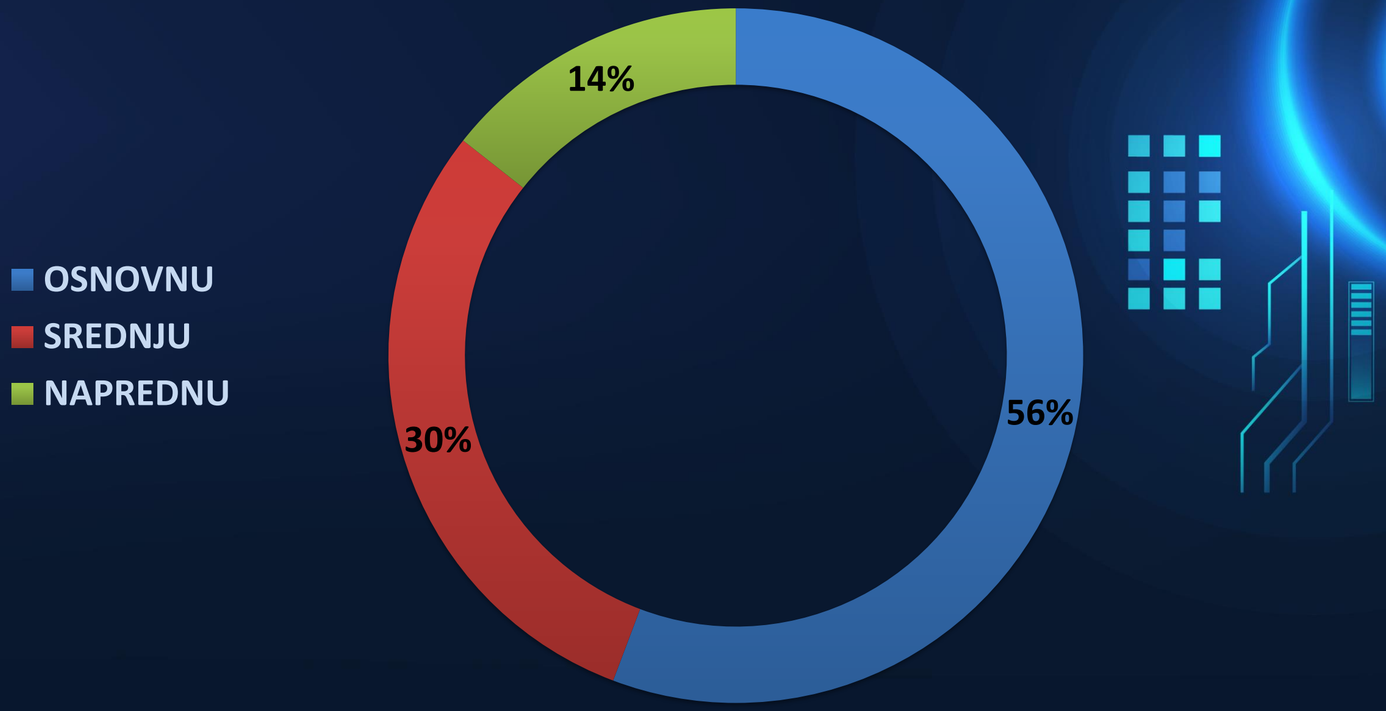
HGK
HRVATSKA GOSPODARSKA KOMORA

Ako ste kategorizirani, u koji sektor pripadate prema Zakonu?



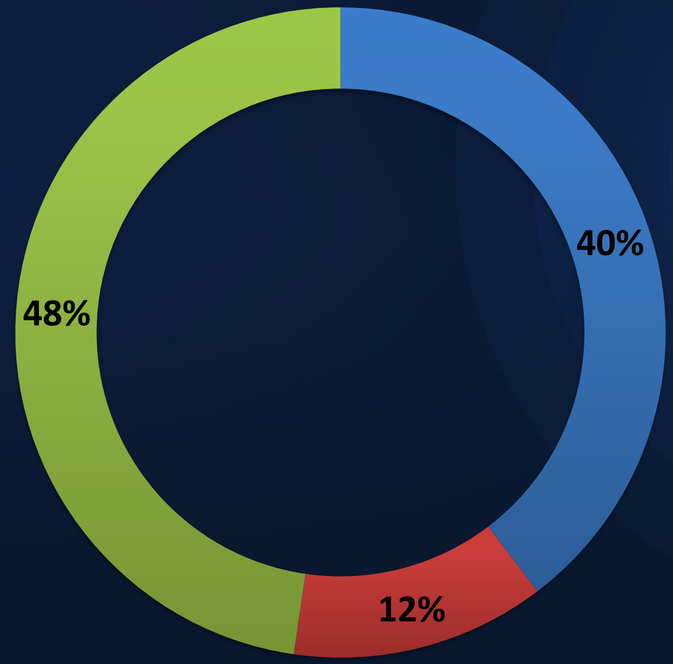
4. Koju razinu sigurnosnih mjera ste obvezni implementirati?

Velik raspon dodijeljenih razina (osnovna–napredna) pokazuje da se Zakon primjenjuje na organizacije vrlo različitih kapaciteta, što stvara jasnu potrebu za prilagođenim pristupom implementaciji i edukaciji.



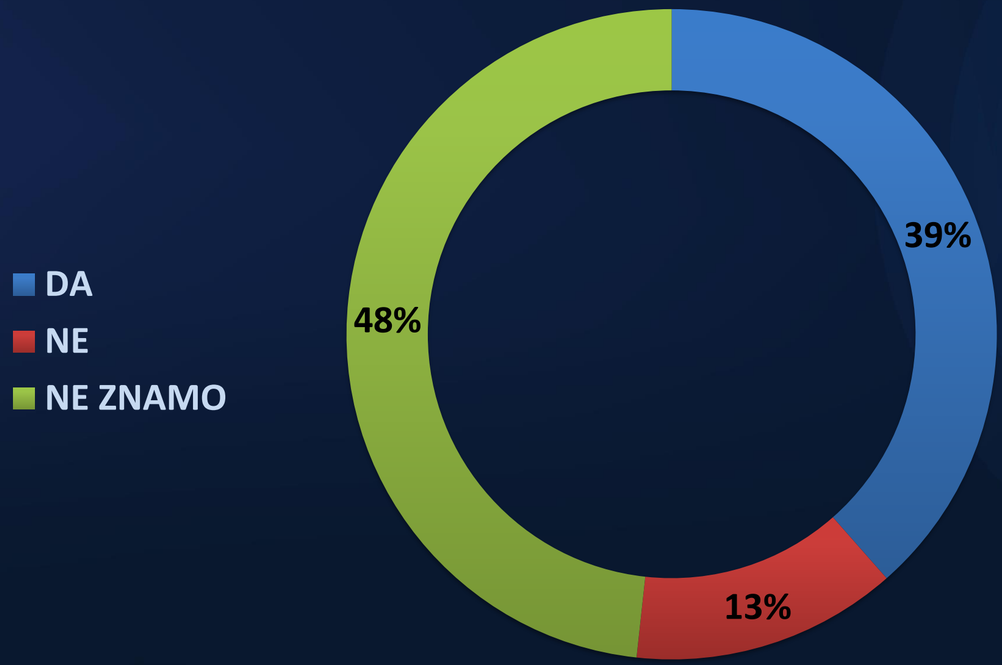
5. Surađuje li Vaša tvrtka s organizacijama koje su kategorizirane?

Značajan broj tvrtki posluje s kategoriziranim subjektima, što povećava važnost sigurnosti dobavnog lanca i jasno pokazuje da se rizik prelijeva iz jedne organizacije na drugu.



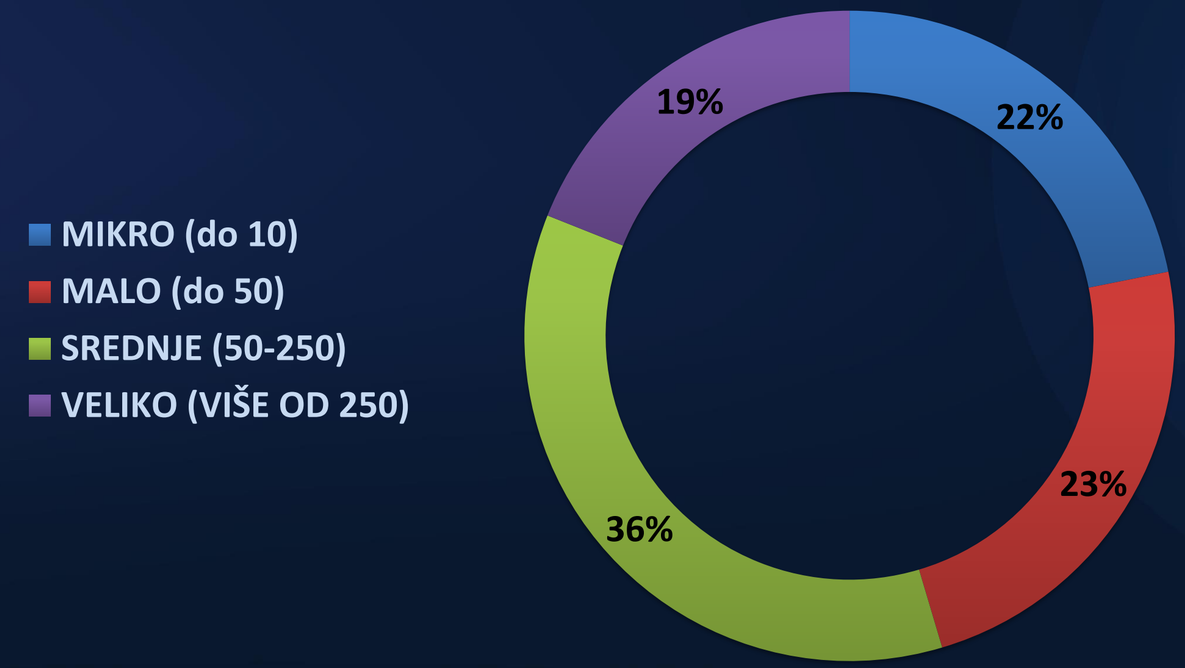
6. Ako još niste kategorizirani, očekujete li da biste mogli biti u budućnosti?

Tvrtke očekuju da će možda ući u sustav obveza, ali bez jasnih informacija. To je indikator da tržište rapidno postaje svjesnije obveza, ali ne i dovoljno pripremljeno.



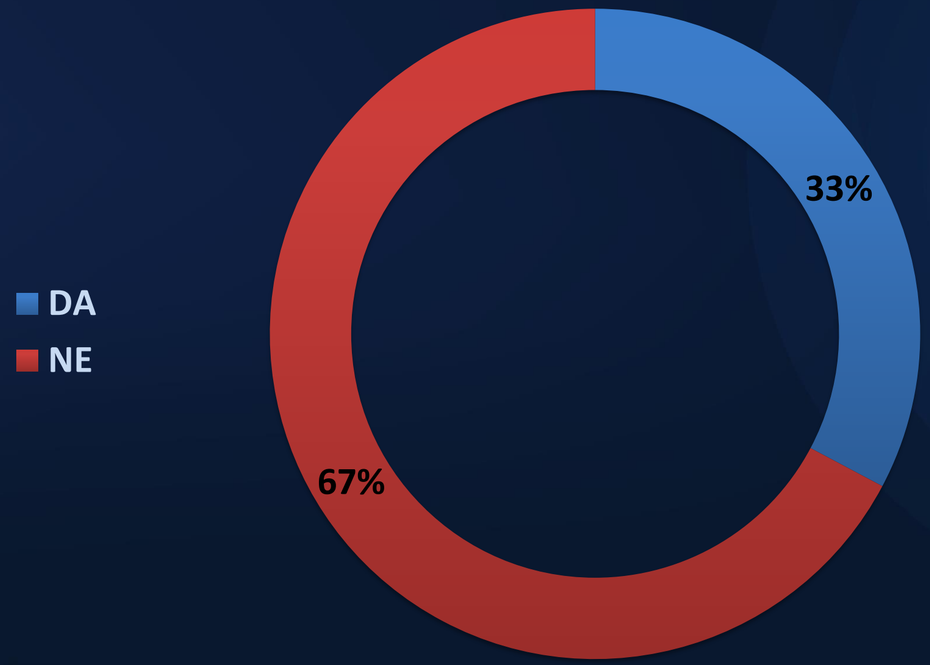
7. Koliko zaposlenika ima Vaša organizacija?

Uzorak uključuje sve veličine, ali struktura odgovora sugerira da srednje i male tvrtke imaju najveću potrebu za podrškom jer najčešće nemaju formalizirane sigurnosne funkcije.



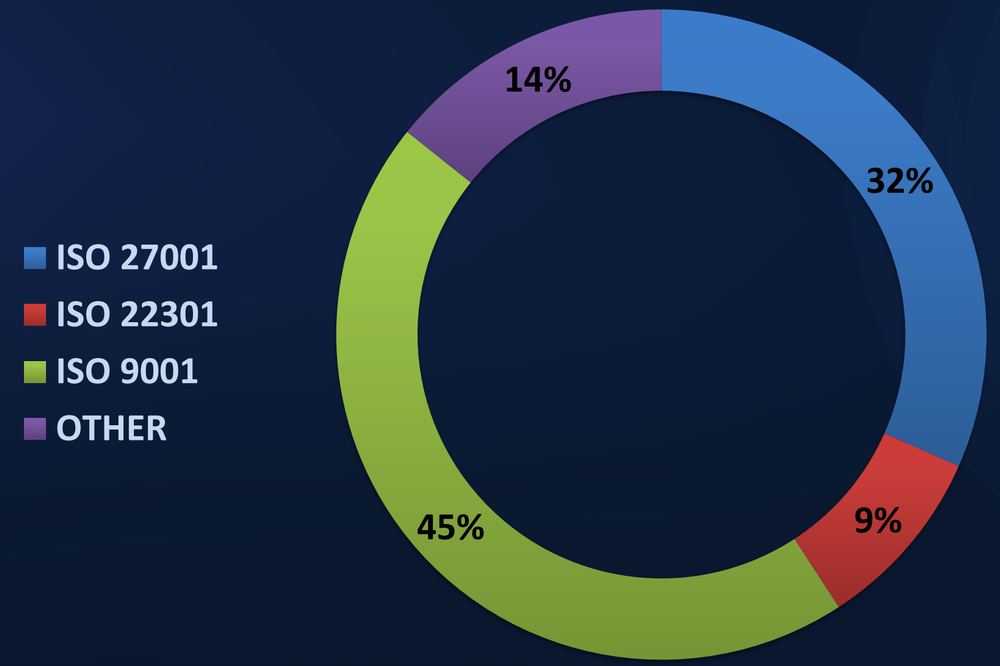
8. Imate li implementirane ISO standarde vezane uz sigurnost i kontinuitet poslovanja?

Samo manji dio ima implementirane sigurnosne ISO standarde, što potvrđuje da većina tvrtki nije dosegnula zreliju razinu upravljanja informacijskom sigurnošću.



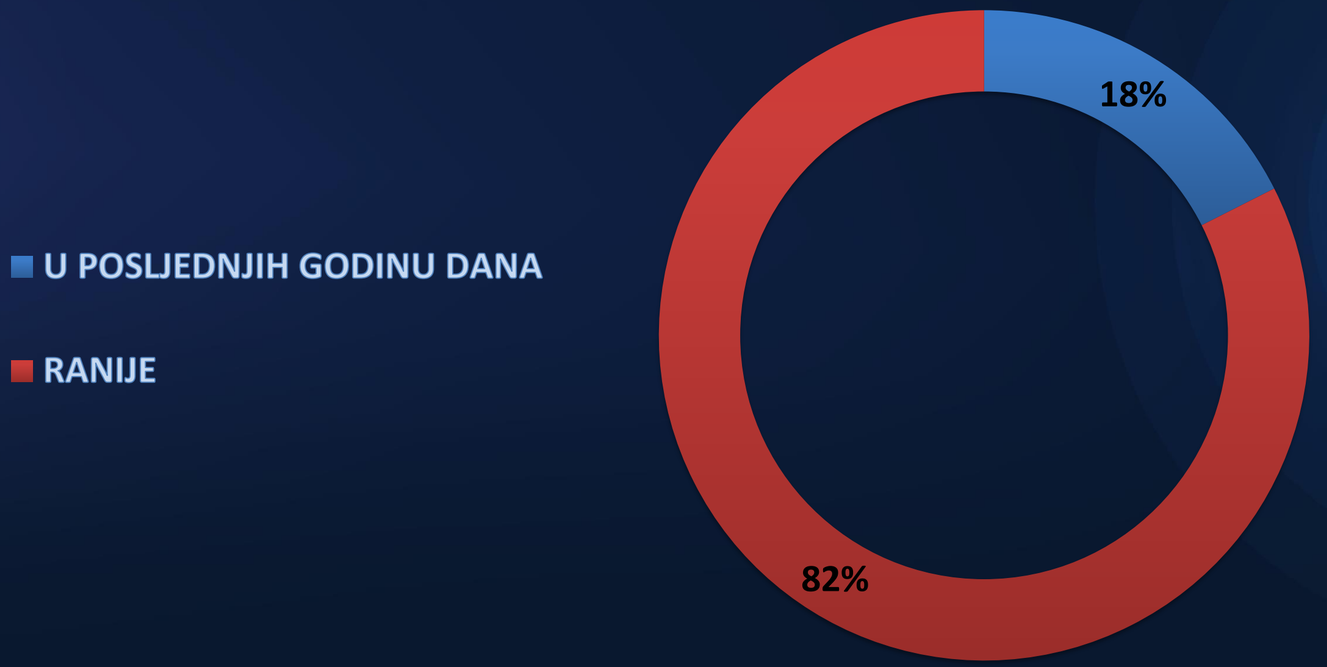
9. Ako DA, koje standarde primjenjujete? (moguće višestruki odabir)

ISO 9001 dominira, što znači da je sigurnost i dalje sekundarna u odnosu na kvalitetu.



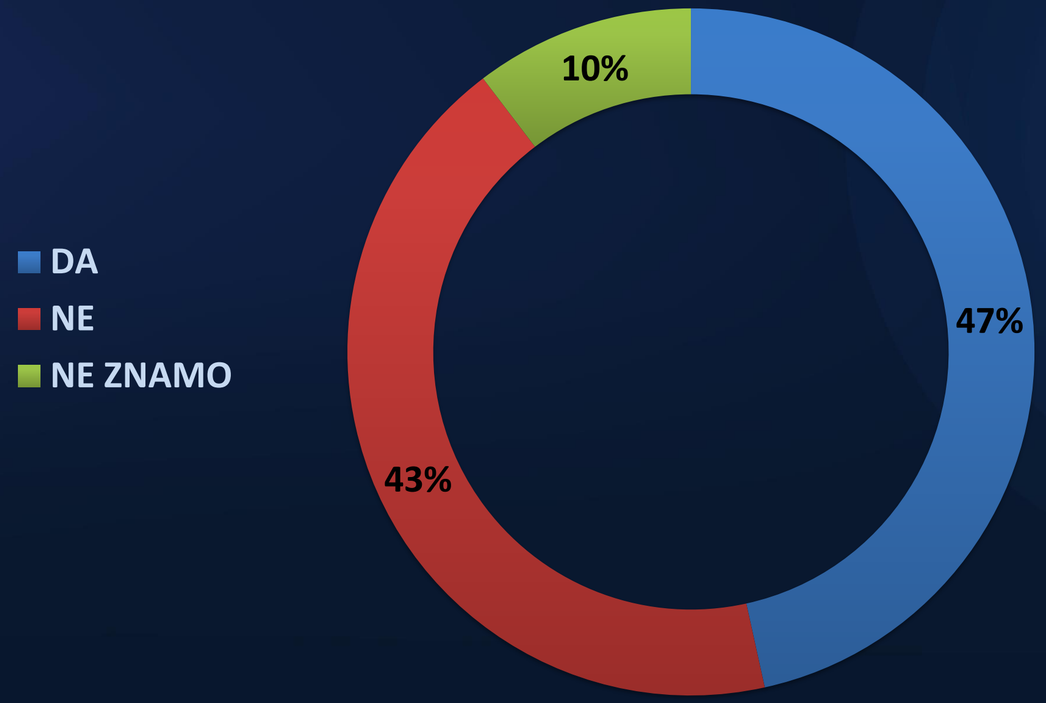
10. Kada su implementirani?

Malo je novih implementacija, što upućuje na stagnaciju i spor napredak u formalizaciji sustava sigurnosti.

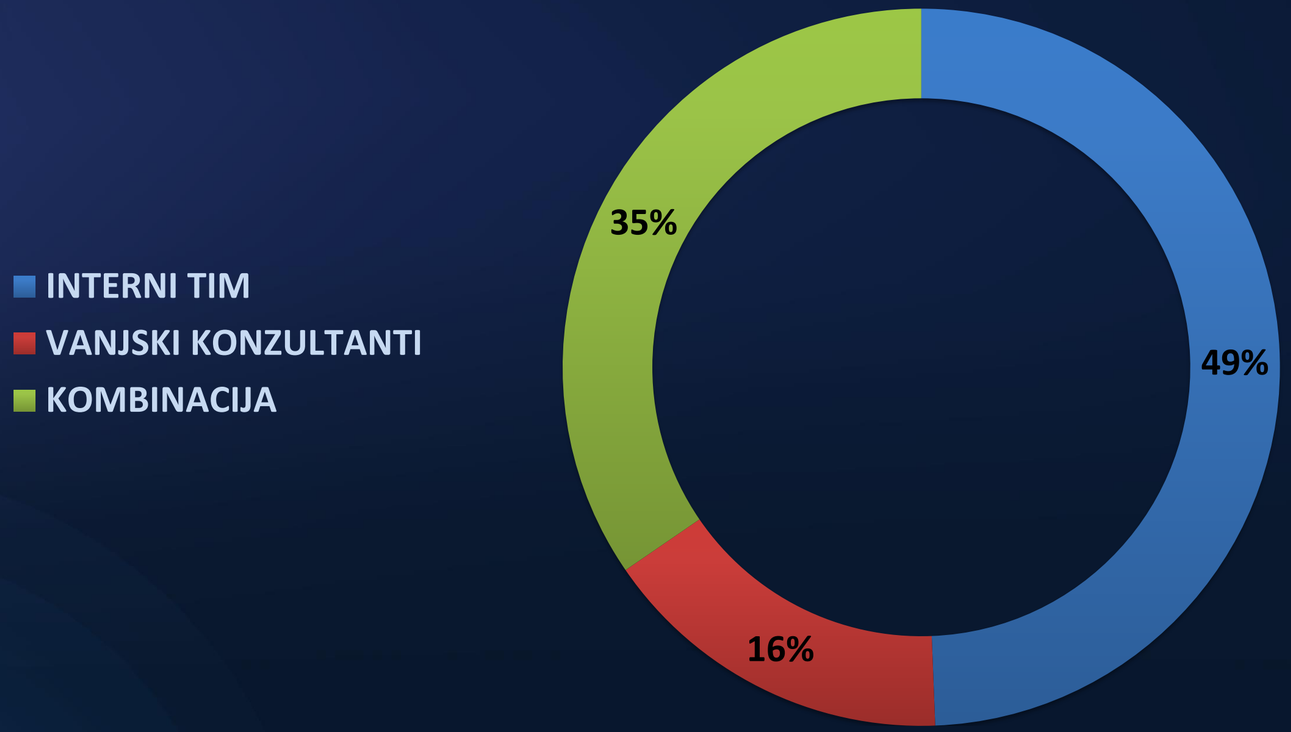


11. Provodite li procjene rizika u području infomacijske sigurnosti?

Mnoge tvrtke rade procjene rizika, no često ih provode interno — što pokazuje određeni kapacitet, ali i rizik od nedovoljne stručnosti, pogotovo bez formalne edukacije.

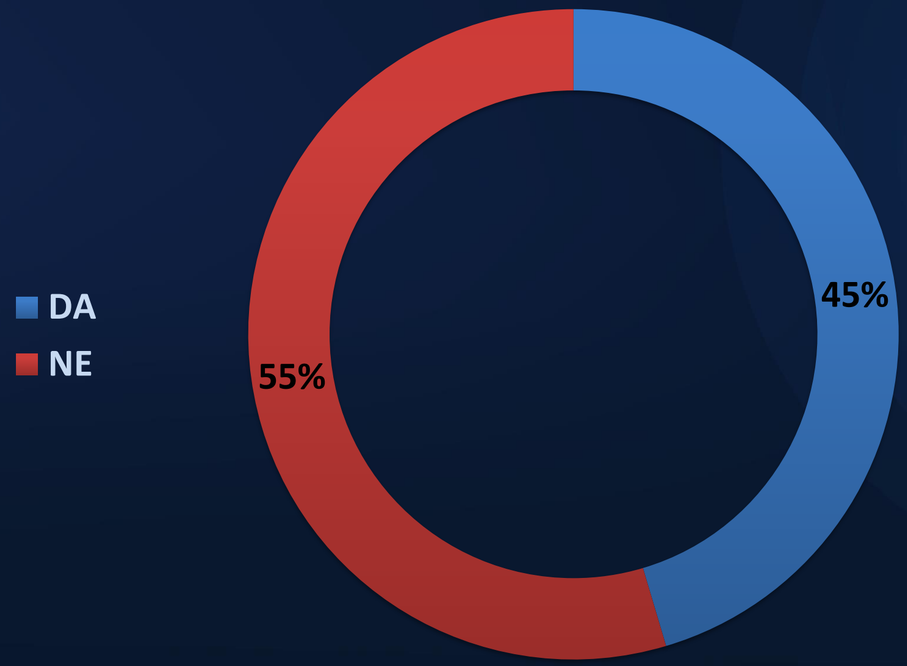


12. Ako DA, tko ih provodi?

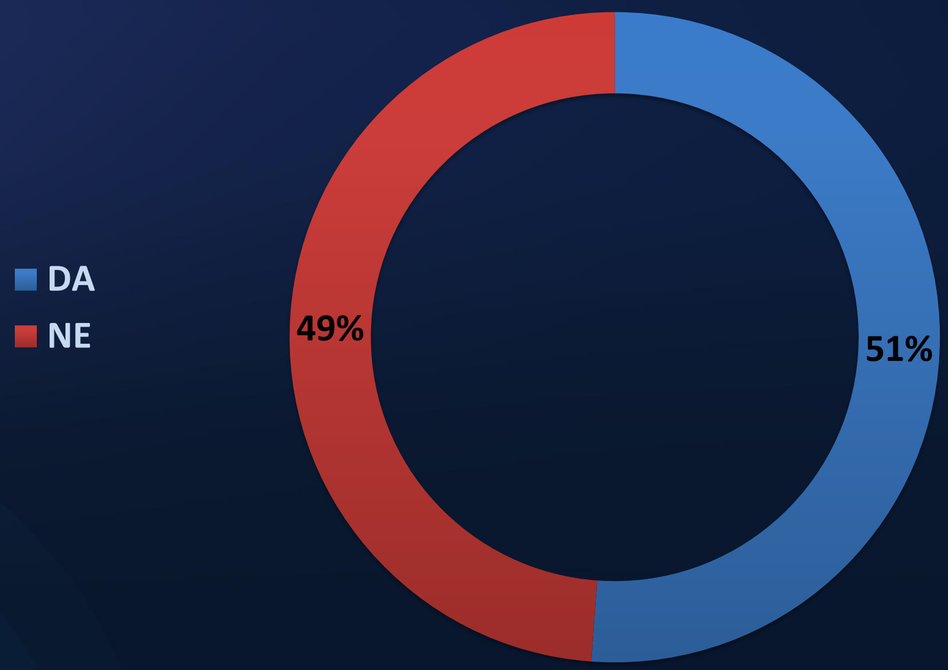


13. Ima li tvrtka osobu koja je formalno zadužena za kibernetičku sigurnost?

Velik broj zaposlenika preuzima funkciju odgovorne osobe uz svoj osnovni posao. To stvara preopterećenje i povećava rizik jer sigurnost nije primarna funkcija, već dodatna obaveza.

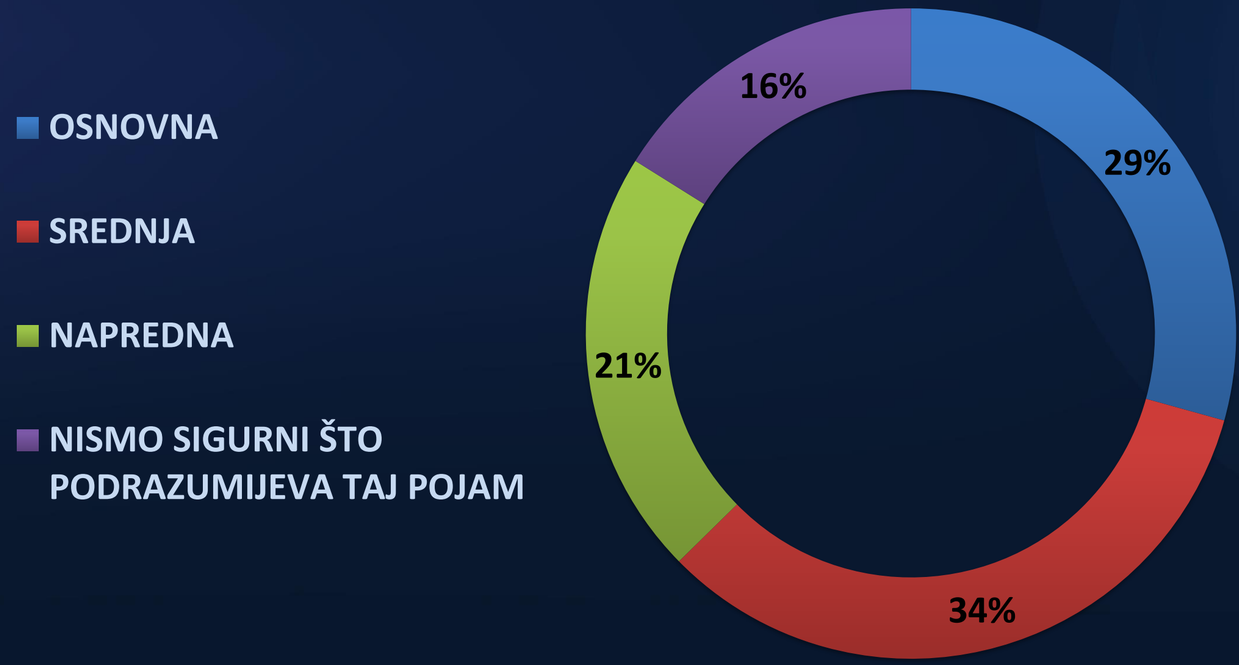


14. Obnašate li Vi ulogu odgovorne osobe za područje informacijske/kibernetičke sigurnosti?



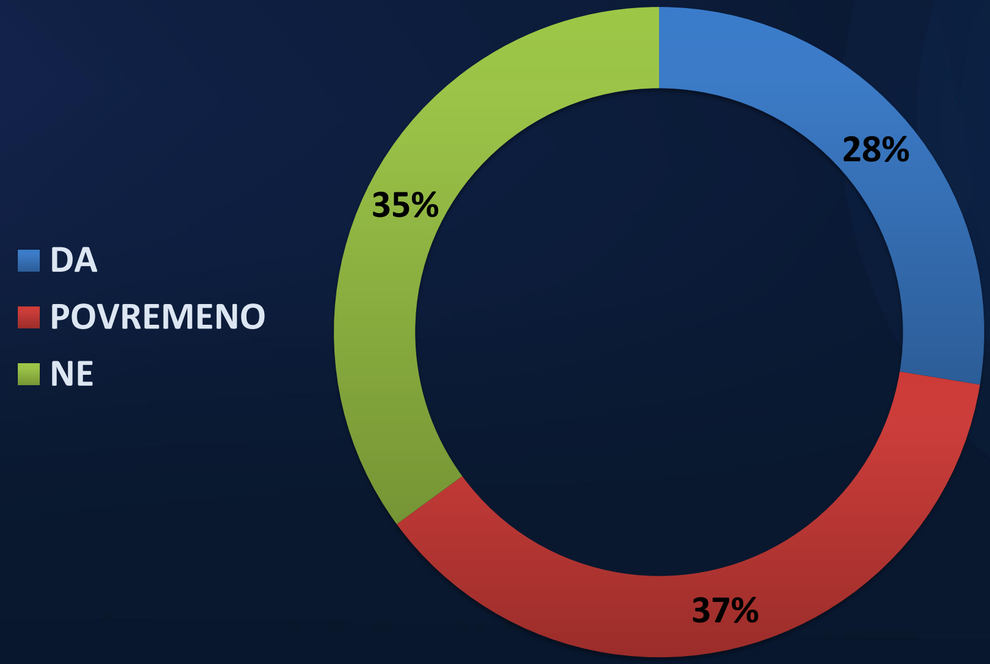
15. Kako biste opisali razinu tzv. „kibernetičke higijene” u tvrtki (osnovna informatička sigurnosna praksa)?

Srednja razina higijene je najčešća, ali zabrinjava broj onih koji ne razumiju pojam, što otkriva temeljni nedostatak sigurnosne kulture i potrebu za osnovnim edukacijama.

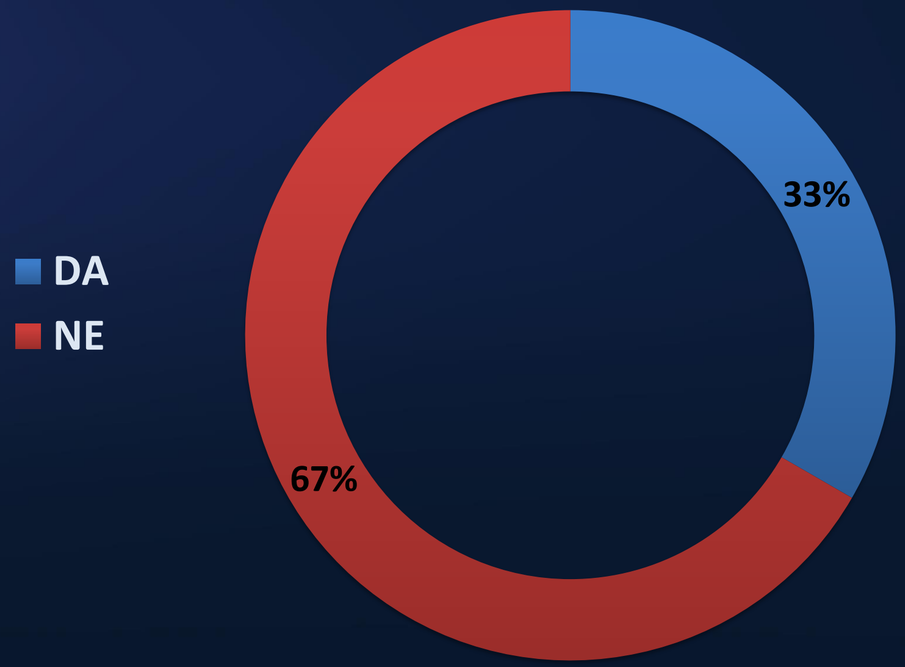


16. Provodite li plan edukacije zaposlenika o digitalnim prijetnjama i sigurnim prijetnjama?

Edukacije se provode, ali često ad hoc. Nedostatak kontinuiteta kompromitira učinak i ne gradi trajnu otpornost ljudi kao najčešće mete napada.

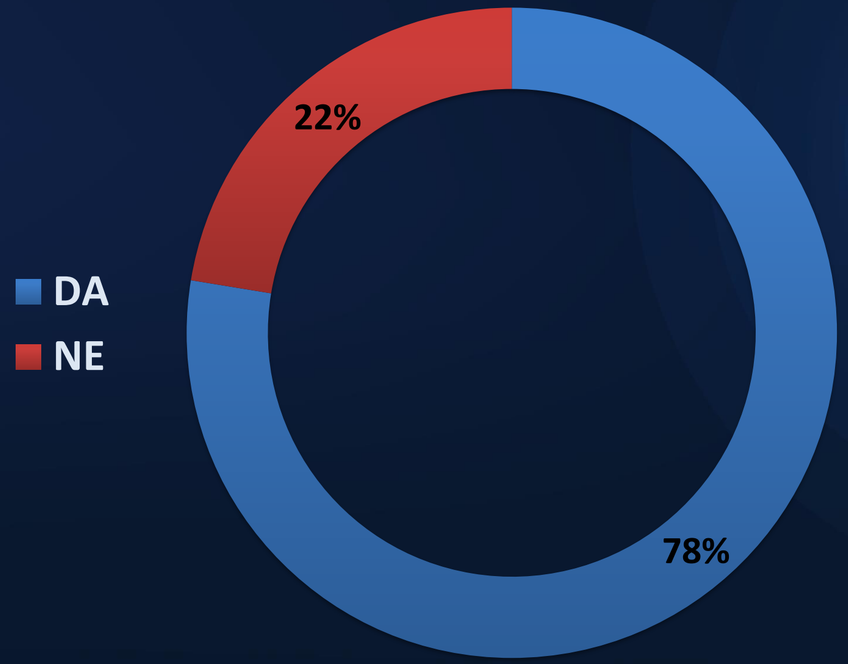


17. Postoji li plan odgovora na incidente?



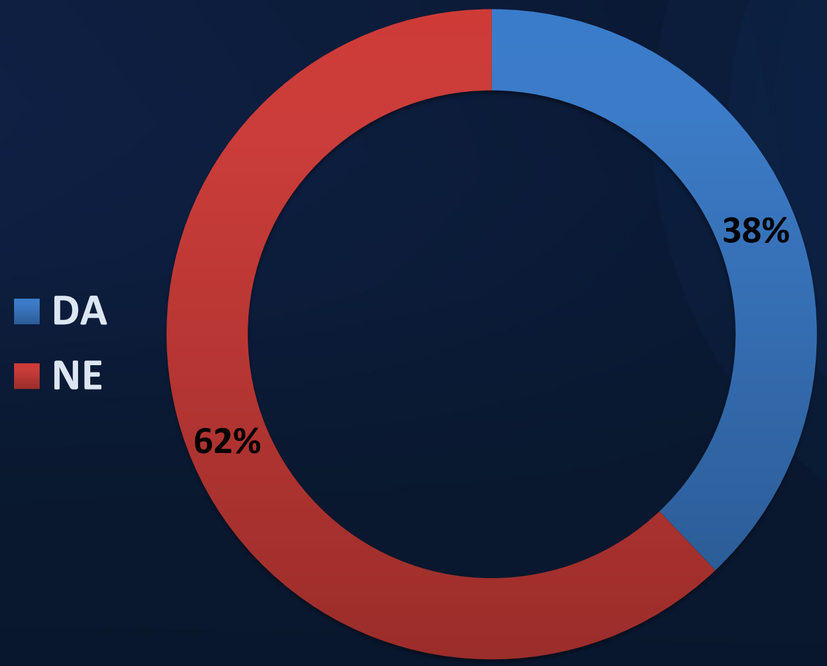
18. Ako DA, postoji li definiran tim i protokol za postupanje kod incidenata?

Planovi postoje, ali većina ih nije detaljna niti operativno razrađena. Nedostatak definiranih timova pokazuje da se organizacije oslanjaju na improvizaciju u slučaju incidenta.

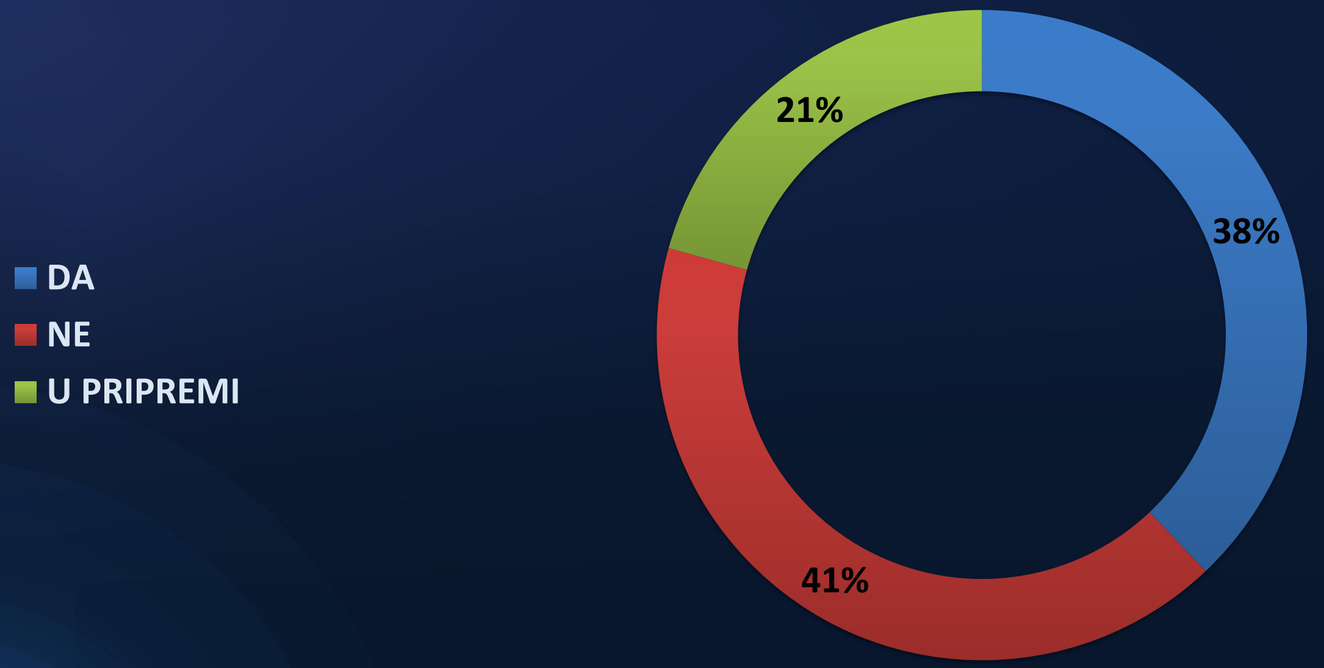


19. Provjeravate li sigurnost svog dobavnog lanca (partnera, dobavljača, IT pružatelja)?

Manji dio organizacija evaluira sigurnost partnera, što potvrđuje da dobavni lanac ostaje jedno od najslabijih mjesta i najvećih rizika.

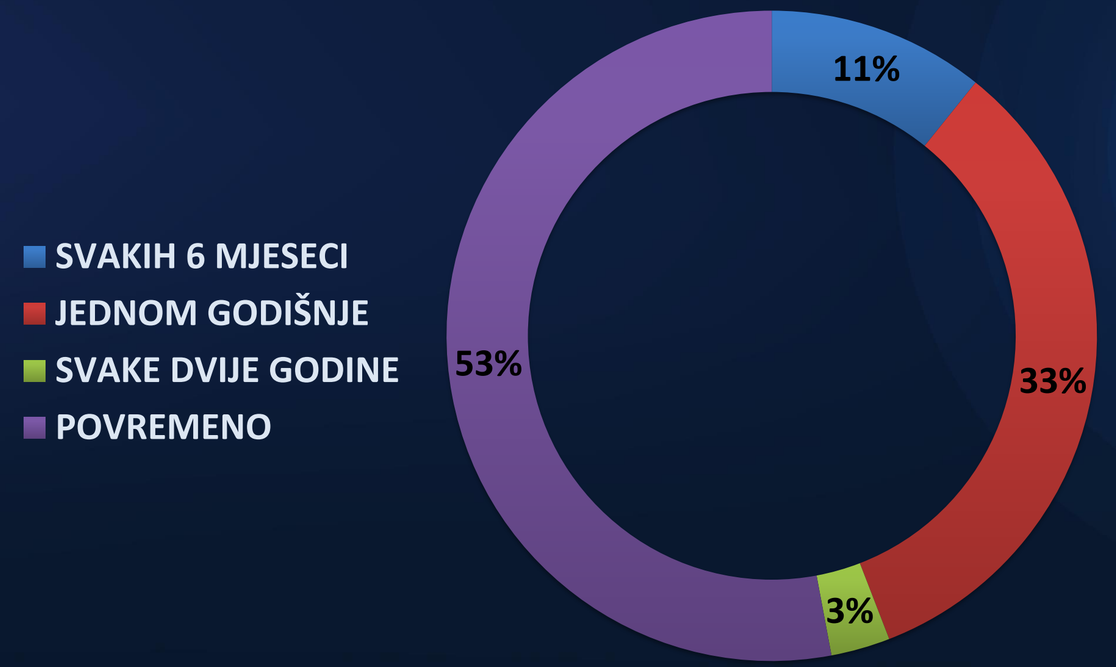


20. Imate li plan kontinuiteta poslovanja i oporavka od nepredviđenih događaja (disaster recovery)?

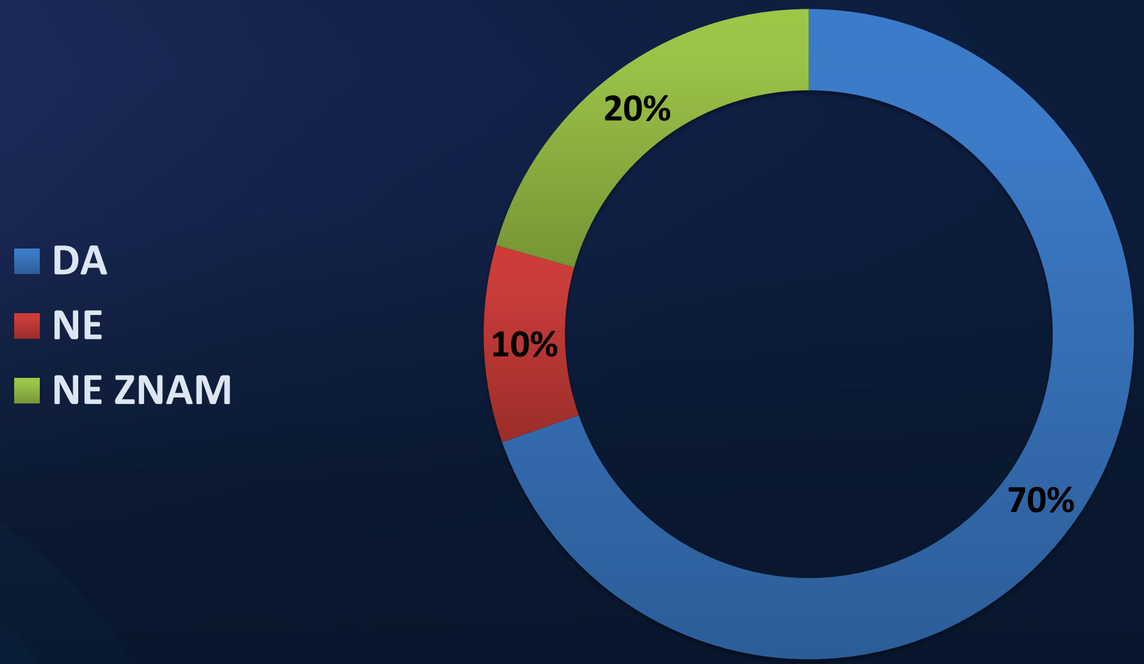


21. Ako DA ili U PRIPREMI, koliko često ga testirate?

Dio organizacija ima planove kontinuiteta, ali njihov sadržaj nije uvijek usklađen s modernim kibernetičkim prijetnjama. Često su planovi neaktualni ili ih se ne testira.

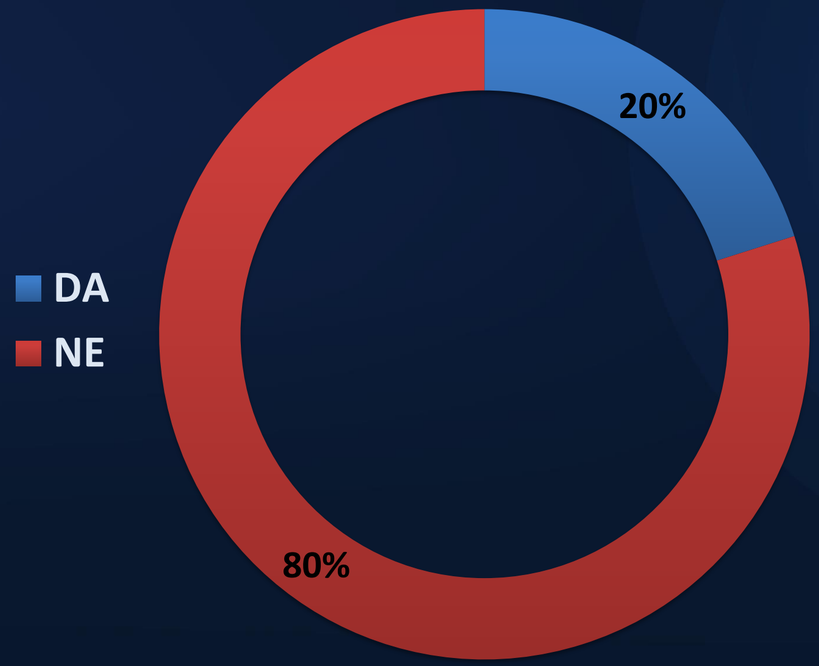


22. Uključuje li taj plan oporavak od potencijalnih kibernetičkih incidenata?

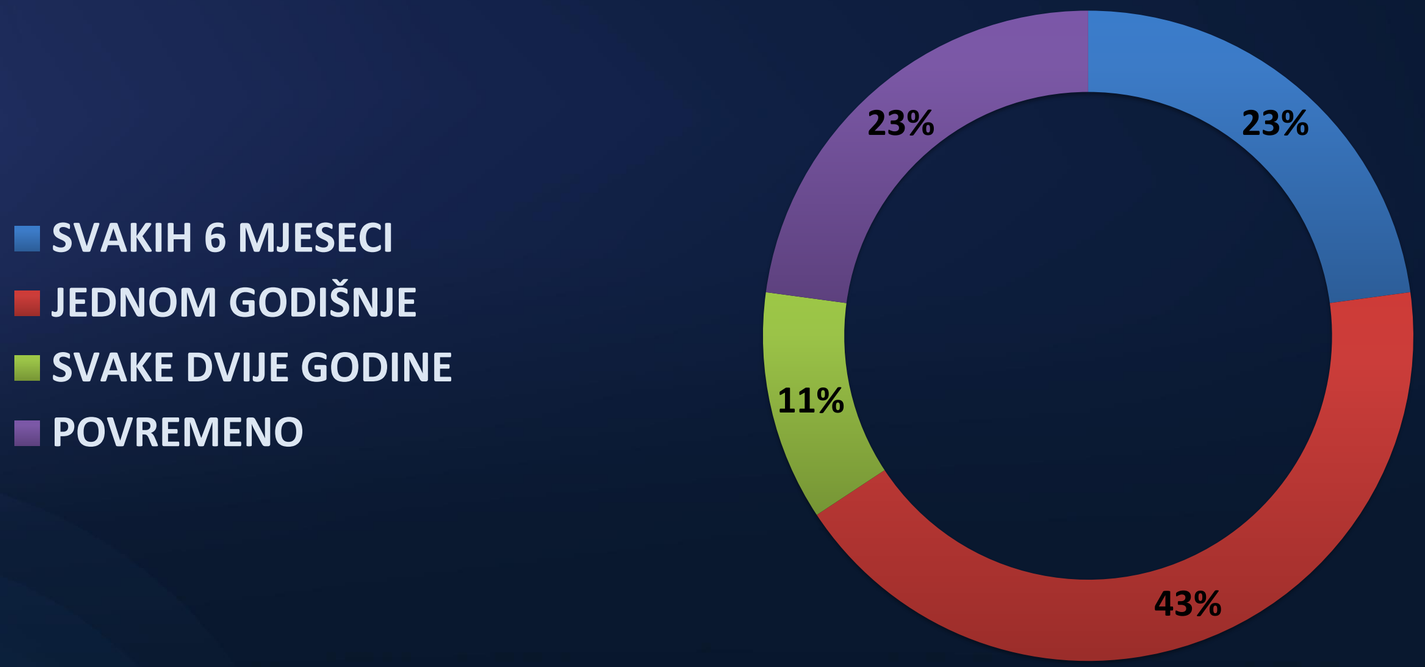


23. Provodite li testiranja i simulacije kibernetičkih incidenata?

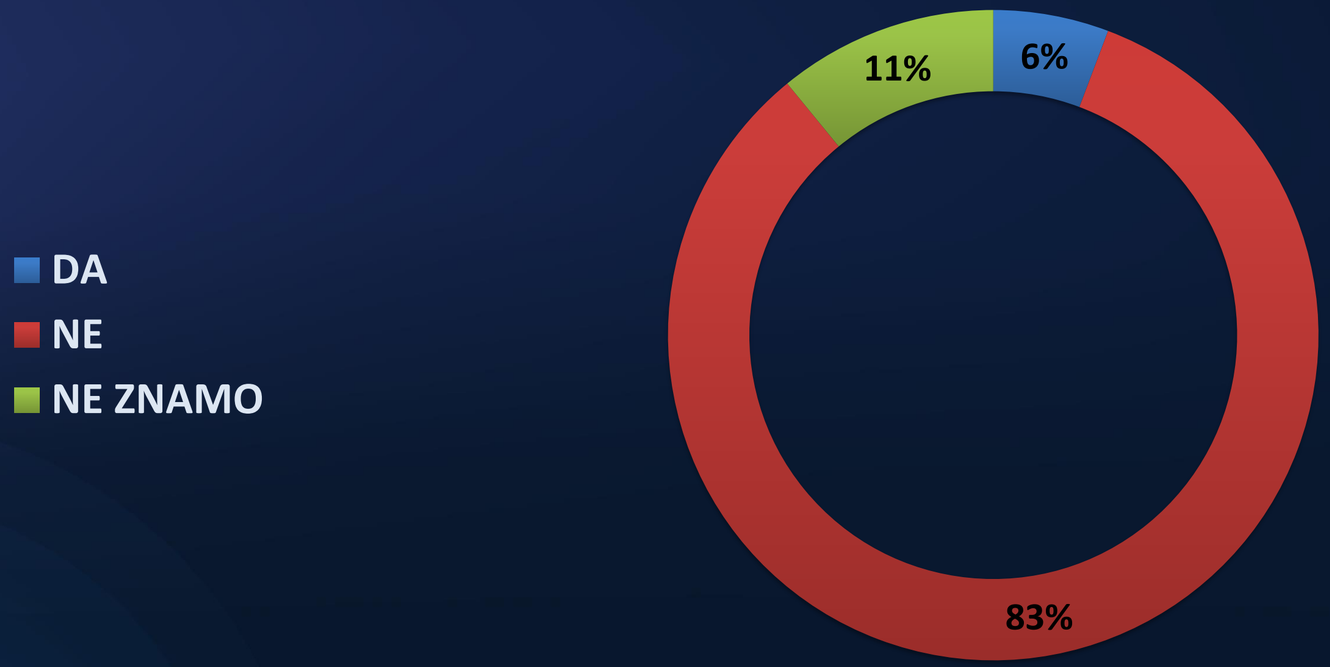
Simulacije provodi mali broj organizacija. Treninzi „na suho“ gotovo ne postoje, što ukazuje na vrlo nizak stupanj operativne spremnosti.



24. Ako DA, koliko često?



25. Je li Vaša organizacija bila žrtva kibernetičkog napada u posljednjih 12 mjeseci?

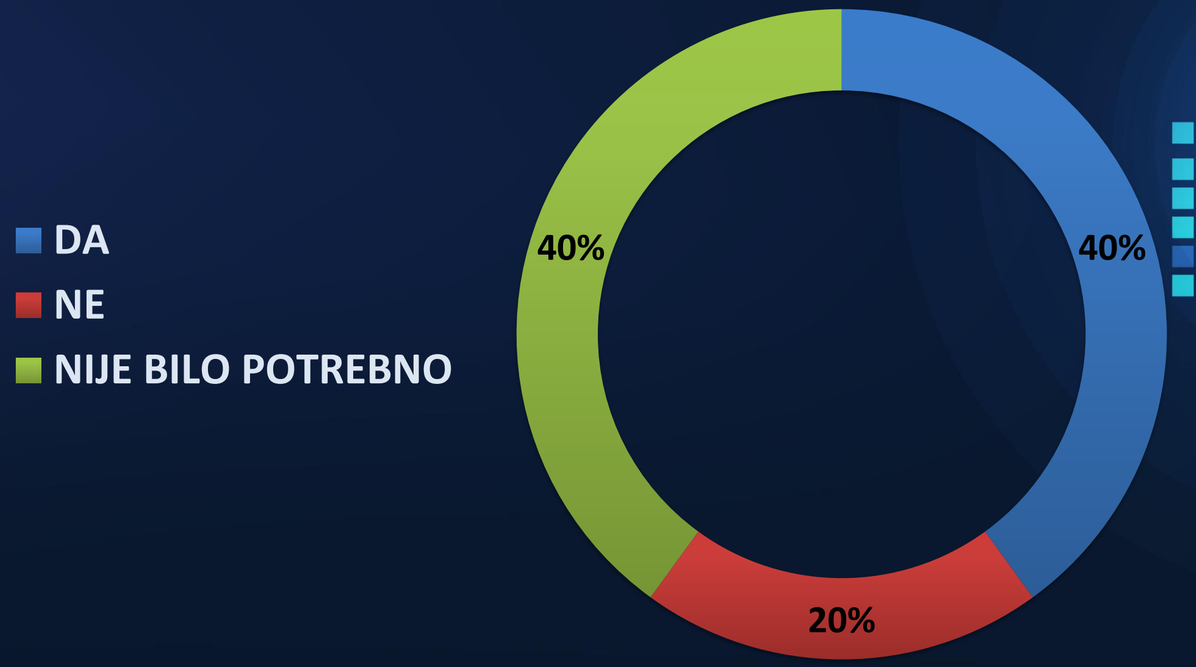


26. Ako DA, o kojoj vrsti napada se radilo? (moguće višestruki odabir)

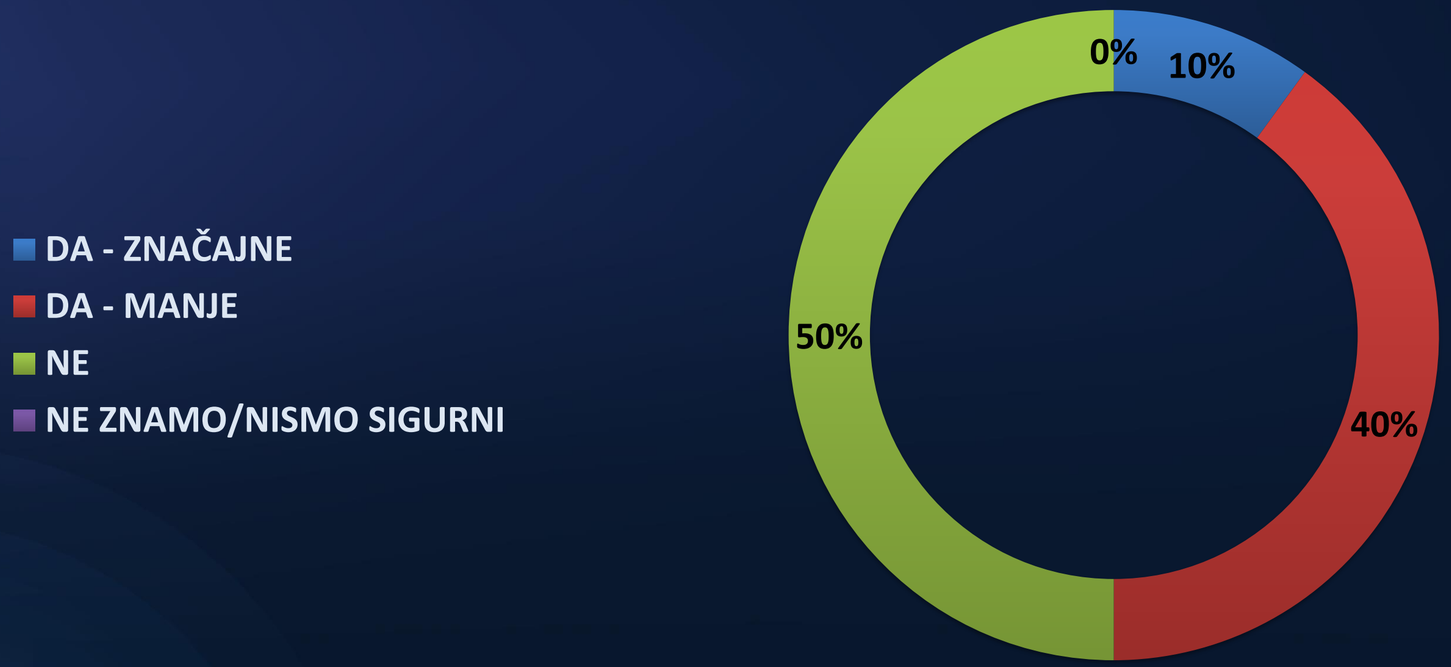
27. Jeste li incident prijavili nadležnim tijelima (CERT, AZOP, regulator itd.)?

Nizak broj prijavljenih napada može ukazivati na dvije stvari:

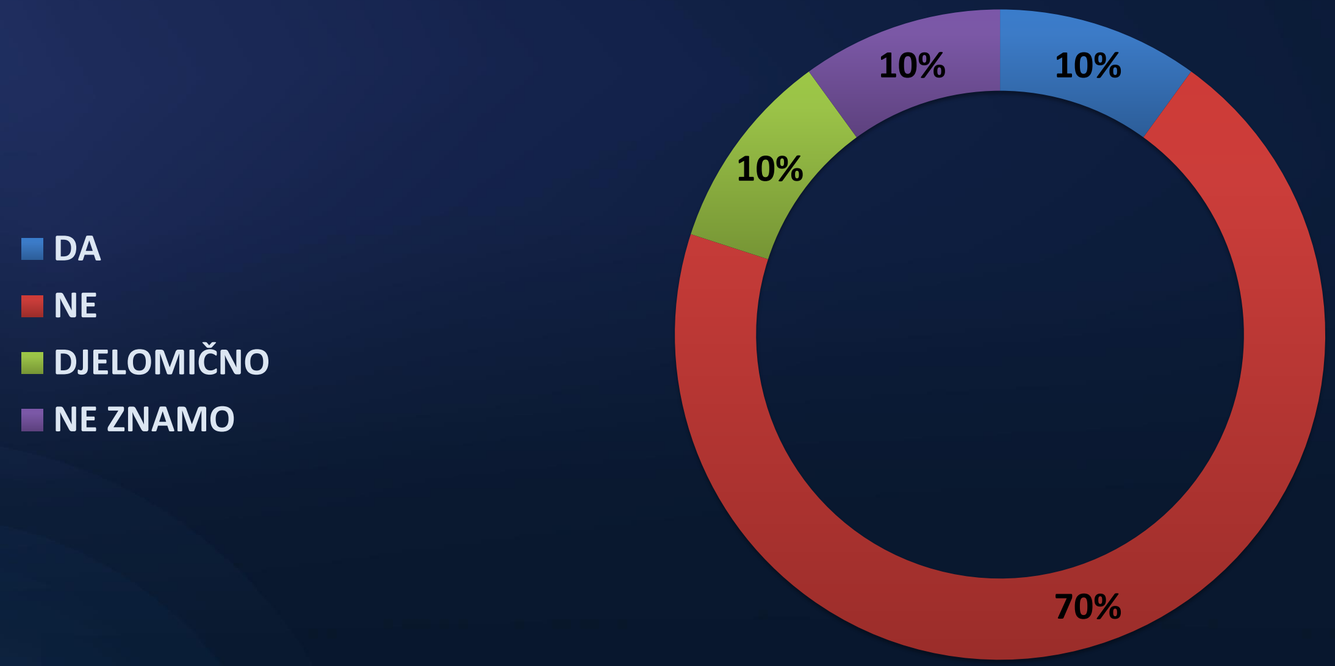
- ili je stvarna učestalost mala,
- ili organizacije ne prepoznaju da je do napada došlo.



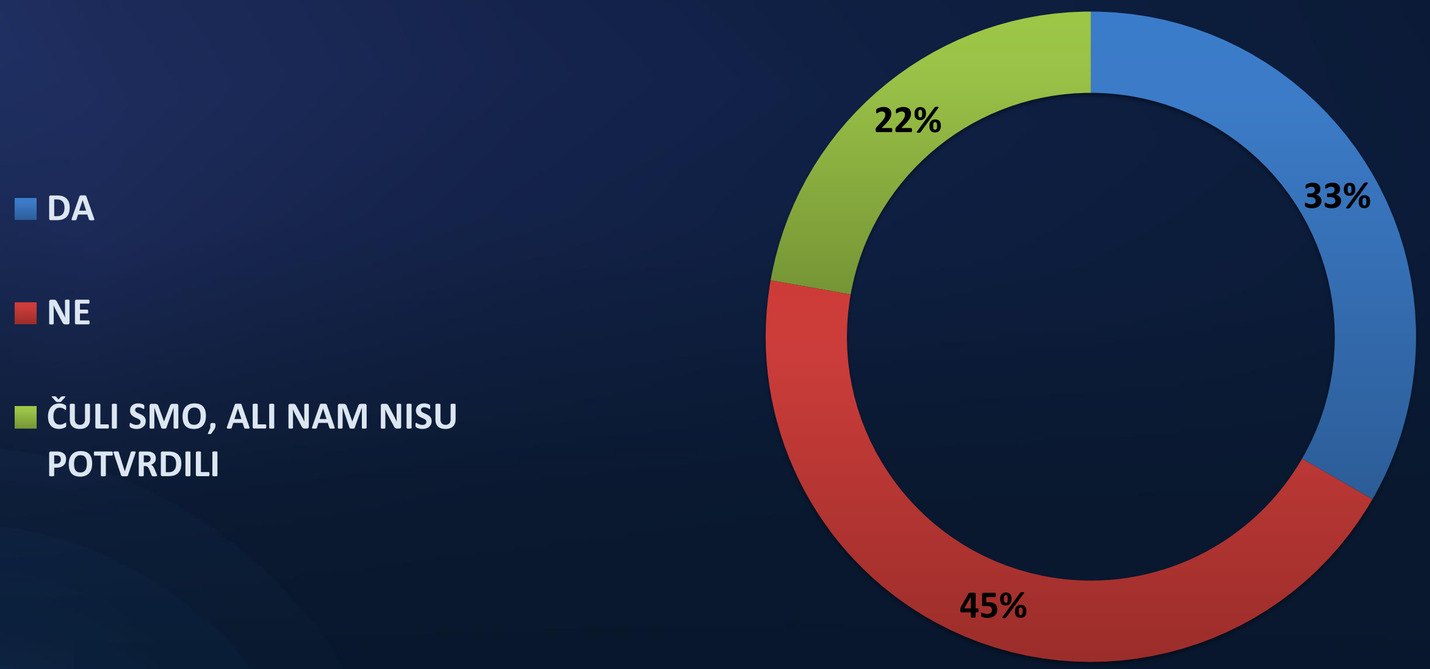
28. Je li napad imao financijske ili operativne posljedice za Vašu organizaciju?



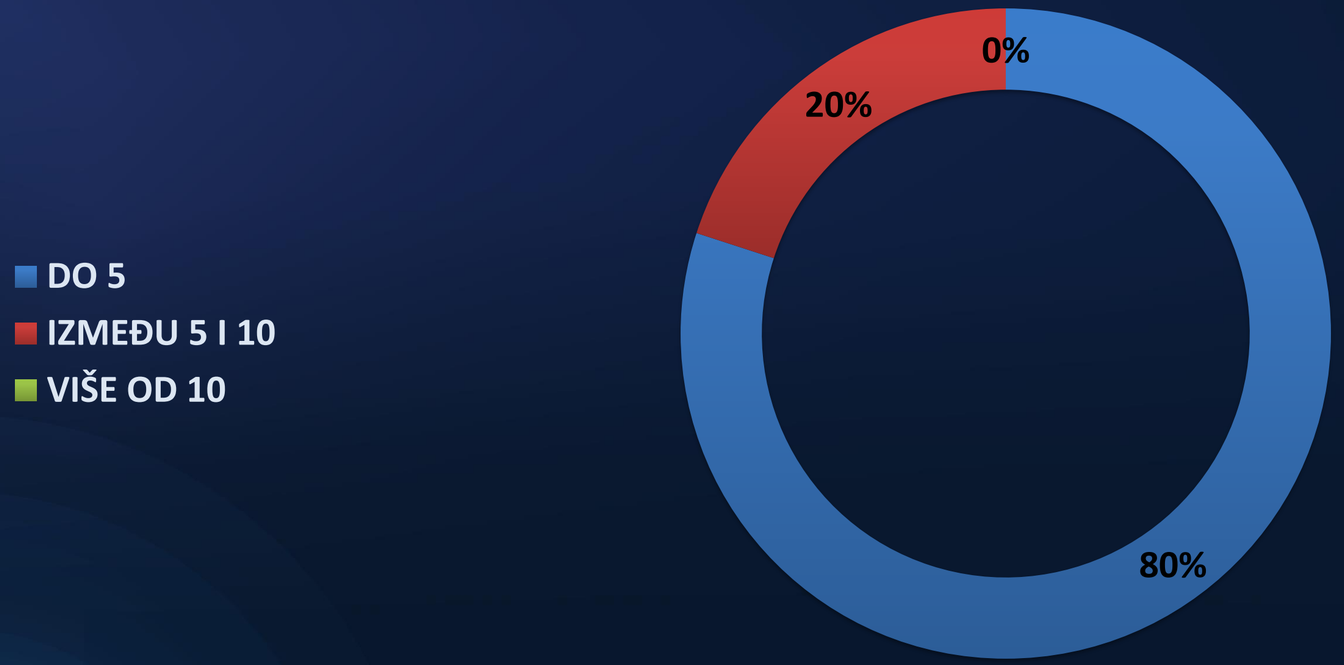
29. Je li napad utjecao na dostupnost usluga ili povjerljivost podataka?



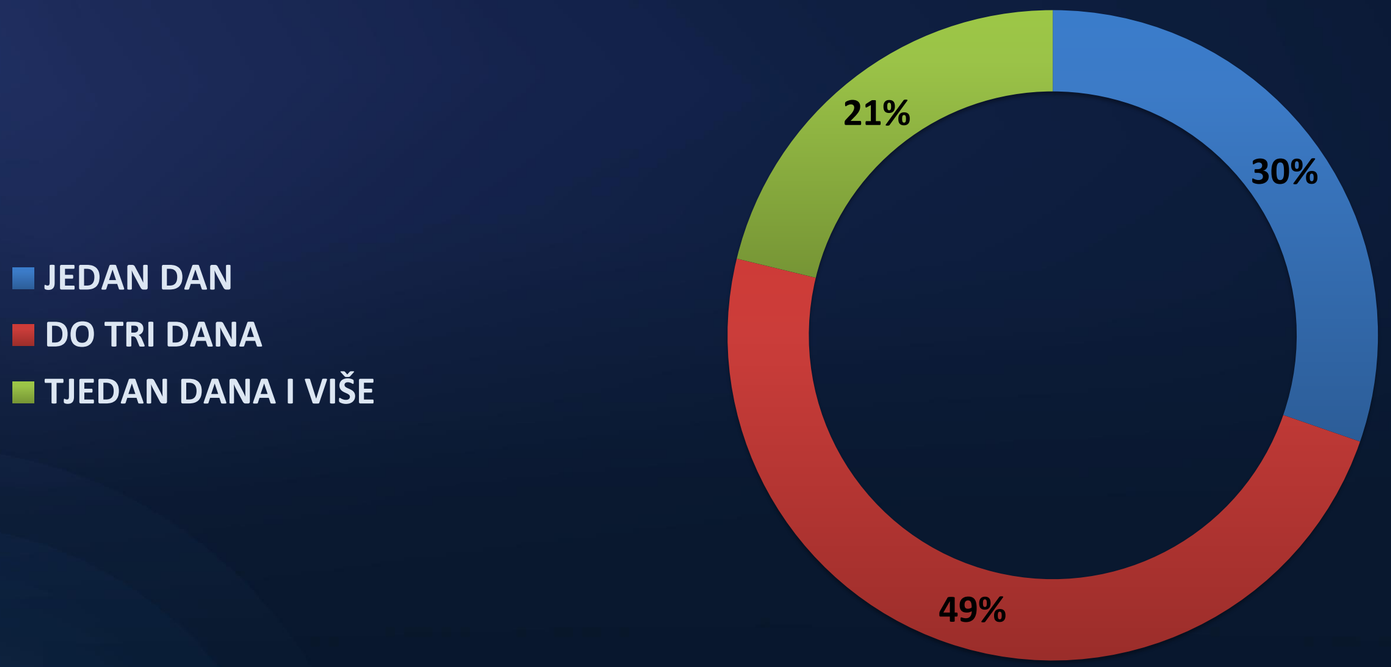
30. Jeste li upoznati s uspješnim napadima na Vaše kupce ili dobavljače?



31. Ako DA ili ČULI SMO, možete li procijeniti broj takvih situacija u posljednjih godinu dana?

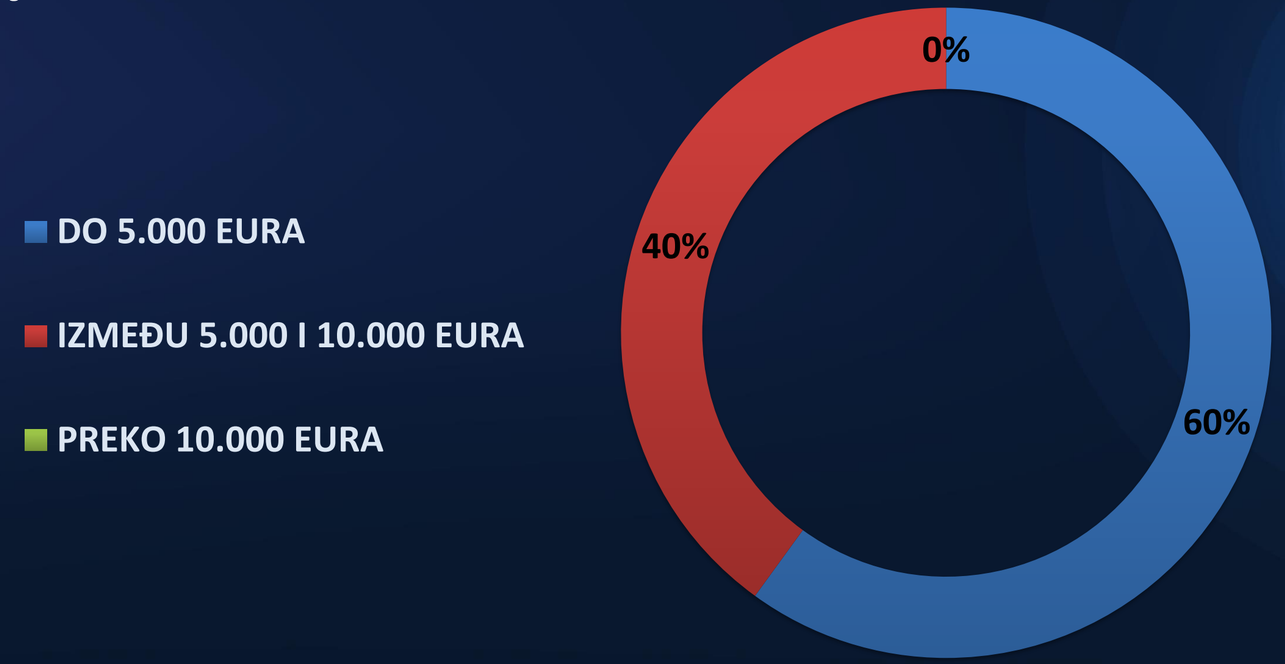


32. Možete li procijeniti koliko su takve situacije utjecale na zastoj ili otežano poslovanje?

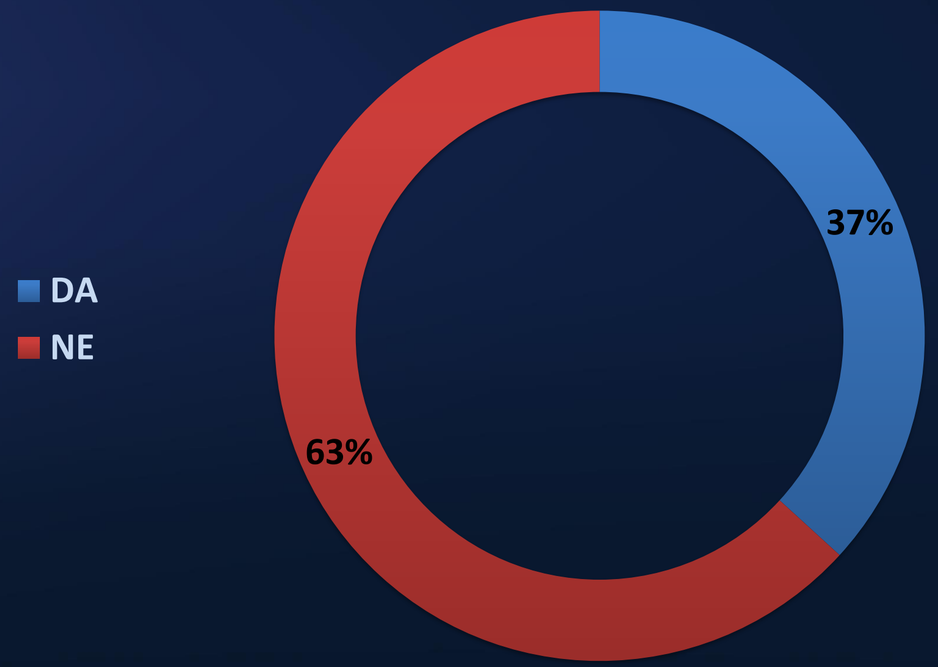


33. Možete li procijeniti koliko su takve situacije uzrokovale financijskih gubitaka?

Incidenti kod partnera uzrokuju kratkoročne prekide poslovanja. Iako posljedice nisu visoke, takvi prekidi pokazuju da bi ozbiljniji napadi imali znatno veći utjecaj.

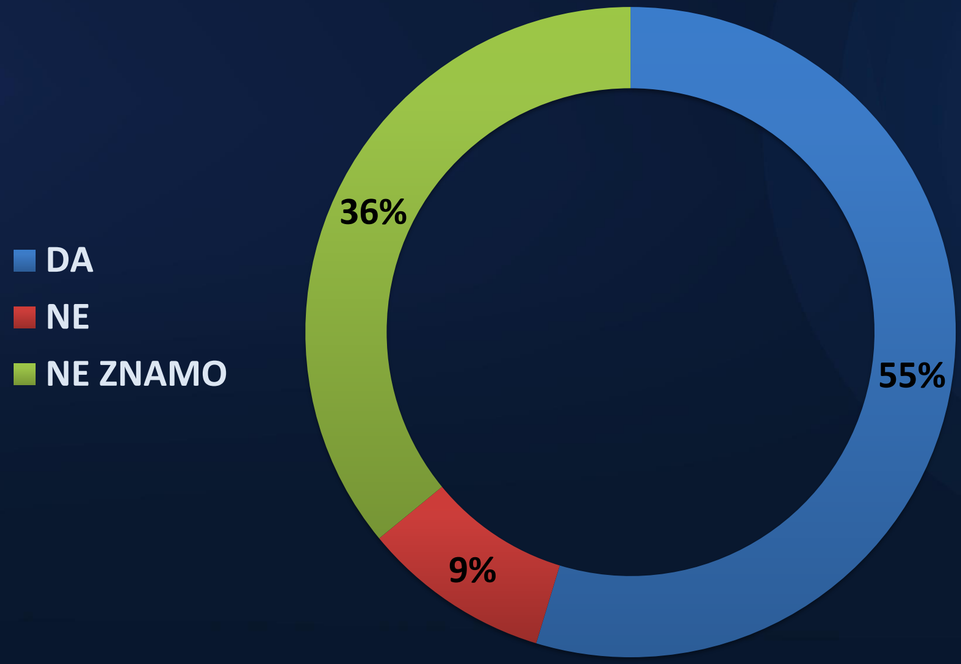


34. Imate li formalno usvojene sigurnosne politike i procedure?



35. Ako DA, uključuju li one mjere iz čl. 30 Zakona o kibernetičkoj sigurnosti?

Dio tvrtki ima formalizirane politike, ali njihov sadržaj nije uvijek usklađen sa Zakonom. Ovo pokazuje starije, zastarjele procedure koje treba modernizirati.



OPĆI ZAKLJUČCI - TRENDOVI I IZAZOVI

- U 2025. prvi put je vidljivo sustavnije mjerenje kibernetičke sigurnosti (procjene rizika, rast formalnih politika i procedura).
- Dio organizacija uvodi standarde ISO 27001 i/ili 22301, no većina još nema cjelovito uspostavljen sustav.
- Postupanje s incidentima se postupno formalizira – pojavljuju se definirani timovi i protokoli.
- Kibernetička sigurnost se i dalje češće promatra operativno nego strateški.
- Testiranja, simulacije napada i vježbe i dalje se provode u vrlo ograničenom opsegu.

OPĆI ZAKLJUČCI - TRENDOVI I IZAZOVI

- Kibernetička higijena je uglavnom na osnovnoj do srednjoj razini (lozinke, ažuriranja, edukacije ostaju slabosti).
- Vidljiv je pozitivan trend profesionalizacije i formalizacije u odnosu na 2024. godinu.
- Organizacije sve češće prepoznaju vlastitu razinu zrelosti, što ukazuje na rast svijesti.
- Razumijevanje obveza iz Zakona o kibernetičkoj sigurnosti je jasnije nego 2024., ali i dalje nedovoljno.
- Glavni izazovi ostaju:
    a) nedostatak formalnih sigurnosnih politika
    b) slabo razvijeni mehanizmi upravljanja incidentima
    c) niska razina testiranja
    d) ograničeno razumijevanje regulatornih zahtjeva

HGK
HRVATSKA
GOSPODARSKA
KOMORA

HVALA!