

Mjere kibernetičke sigurnosti – pregled stanja u Europi

Sažetak

Širenje jedinstvenog digitalnog tržišta na globalnoj razini potaknulo je zakonodavce da utvrde uvjete koje dionici u digitalnom okruženju moraju ispuniti kako bi se osigurala kibernetička sigurnost digitalnog poslovnog i društvenog okruženja. Tako je 2016. godine Europska unija uvela u primjenu direktivu NIS (engl. Network and Information Systems) (EK, 2016) koja je u 2022. godini dobila novo izdanje NIS 2 (EK, 2022). Obvezu primjene Direktive NIS 2 imaju zemlje članice Europske Unije (EU), no neke odredbe mogu se primjenjivati i na dionike koji nisu s područja članica Europske Unije, ali posluju sa subjektima koji imaju sjedišta u EU.

Praćenje primjene mjera za osiguranje kibernetičke sigurnosti nužno je radi usmjeravanja pažnje na kritične točke u sustavu zaštite. Što je to europsko tijelo nadležno za statistička istraživanja – EUROSTAT – izvijestilo o stanju u proteklom razdoblju na temu kibernetičke sigurnosti biti će u kratkim crtama prikazano u ovom članku.

Ključne riječi: Eurostat, kibernetička sigurnost, kontrole, NIS 2 direktiva, police osiguranja, svijest zaposlenika

1. UVOD

Digitalno poslovanje ima brojne prednosti, no ono donosi i određene rizike koji nipošto nisu zanemarivi. Radi sustavnog načina djelovanja u skladu sa zajedničkim ciljem, na nivou EU usvojena je Direktiva NIS 2 (EK, 2022).

Kako bi se na razini zemalja EU pratilo kretanje indikatora koji ukazuju jesu li zemlje članice napredovale u ostvarenju zajedničkog cilja i koliko, Eurostat je uveo statistička istraživanja na tu temu. Osiguranje kibernetičke sigurnosti spada u uvjete stabilnog poslovnog digitalnog okruženja u kojem u posljednjem desetljeću djeluje sve veći broj poslovnih subjekata, ali i pojedinaca, građana, koji konzumiraju usluge i proizvode koji su dostupni online.

Motivacija za pisanje ovog teksta proizlazi iz potrebe da se поближе dobije uvid u stanje po zemljama članicama EU i drugim zemljama Europe za pojedine indikatore vezane uz kibernetičku sigurnost. U nastavku članka dat je pregled podataka i kratka analiza o stanju odabranih indikatora. Podaci se uglavnom odnose na 2022. godinu, godinu u kojoj je NIS 2 usvojena. Svaka sljedeća godina uključena u statističko istraživanje trebala bi dati sliku o poboljšanju stanja kibernetičke sigurnosti, a koje se očekuje uvođenjem programa, politika i mjera na nacionalnoj razini te primjenom Direktive NIS 2 u praksi na operativnoj razini.

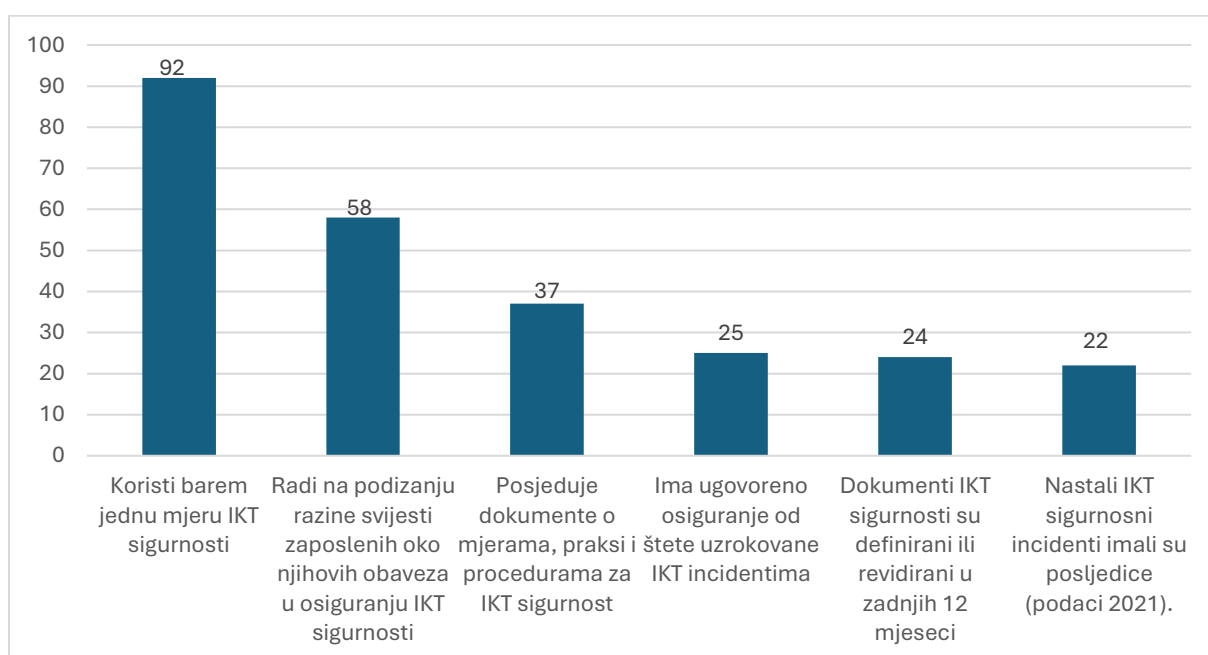
2. PREGLED STANJA KIBERNETIČKE SIGURNOSTI U EUROPI – rezultati i diskusija

Kako je uvodno već opisano cilj rada je dati osnovne informacije o primjeni sigurnosnih mjera zaštite od kibernetičkih napada. Kao osnovni izvor informacija korištena je Eurostat baza podataka o sigurnosti informacijsko komunikacije tehnologije (IKT) u kojoj se prate podaci o sigurnosnoj politici, mjerama, rizicima i svijesti zaposlenika u poslovnim subjektima

i to po veličini poslovnih subjekata prema broju zaposlenih¹ te po djelatnostima² (podaci za 2015., 2019. i 2022. godinu – ovisno o ostalim praćenim atributima).

Također prikupljeni su i obrađeni podaci o sigurnosnim incidentima i posljedicama prema veličini poduzeća uvažavajući kriterij broja zaposlenih³ i po djelatnostima⁴ (podaci za 2019. i 2022. godinu). Recentni podaci govore da u 2022. godini 92 % poslovnih subjekata u EU koristi barem jednu mjeru za IKT sigurnost (Eurostat, 2024), a da u 2021. godini 22 % poslovnih subjekata u EU pati od posljedica kibernetičkih incidenata. U okviru EU oko 25% ispitanih poslovnih subjekata dalo je odgovor da imaju ugovoreno osiguranje od posljedica kibernetičkih incidenata, a čak 58% ispitanih poslovnih subjekata poduzelo je mjere kojima je podignuta svijest zaposlenih o njihovoj ulozi u kibernetičkoj sigurnosti.

Grafikon 1. IKT sigurnost, EU, 2022. godina (% poslovnih subjekata)



Izvor: Eurostat ([isoc_cisce_ra](#)) and ([isoc_cisce_ic](#)), ICT security in enterprises, EU, 2022 (% enterprises)

Uvid u detaljne podatke dobivene statističkim istraživanjem provedenim od EUROSTATATA, prema raznim kriterijima može se izvršiti putem poveznica naznačenih u fusnotama od 1 do 4 na dnu stranice.

¹ Statistika prema veličini gospodarskog subjekta po broju zaposlenih, preuzeto s https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en&category=isoc.isoc_e.isoc_ci_sc, pristupljeno 6. kolovoza 2024.

² Statistika po djelatnostima, preuzeto s https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ran2/default/table?lang=en&category=isoc.isoc_e.isoc_cisc, pristupljeno 6. kolovoza 2024.

³ Statistika prema veličini gospodarskog subjekta po broju zaposlenih, preuzeto s https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en&category=isoc.isoc_e.isoc_ci_sc, pristupljeno 6. kolovoza 2024.

⁴ Statistika po djelatnostima, preuzeto s https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ich2/default/table?lang=en&category=isoc.isoc_e.isoc_cisc, pristupljeno 6. kolovoza 2024.

Tablica 1. IKT sigurnost, EU, 2022. godina (% poslovnih subjekata) – po zemljama EU

	Koristi barem jednu mjeru IKT sigurnosti	Radi na podizanju razine svijesti zaposlenih oko njihovih obaveza u osiguranju IKT sigurnosti	Posjeduje dokumente o mjerama, praksi i procedurama za IKT sigurnost	Ima ugovoreno osiguranje od štete uzrokovane IKT incidentima	Dokumenti IKT sigurnosti su definirani ili revidirani u zadnjih 12 mjeseci	Nastali IKT sigurnosni incidenti imali su posljedice (podaci 2021).
EU	92	58	37	25	24	22
Austrija	92	61	32	27	19	15
Belgija	96	54	34	33	24	23
Bosna i Hercegovina	86	46	26	13	16	21
Bugarska	82	48	22	4	17	11
Cipar	91	52	31	17	21	14
Crna Gora	62	51	15	17	10	23
Češka	92	75	26	12	18	29
Danska	98	70	55	71	37	26
Estonija	86	61	37	9	21	26
Finska	98	67	57	33	43	44
Francuska	93	47	21	40	12	26
Grčka	75	32	18	14	7	18
Hrvatska	85	38	49	7	29	19
Irska	91	75	51	42	35	15
Italija	92	62	48	16	30	16
Latvija	83	50	49	9	40	19
Litva	88	63	34	5	17	16
Luksemburg	86	52	26	31	19	16
Mađarska	79	43	33	5	21	13
Malta	93	60	38	35	26	26
Nizozemska	96	46	44	30	34	30
Norveška	91	58	30	38	21	17
Njemačka	96	68	36	32	24	26
Poljska	93	51	44	14	21	30
Portugal	90	63	54	11	34	11
Rumunjska	86	62	45	7	40	19
Slovačka	86	62	25	10	17	12
Slovenija	87	51	40	8	27	15
Srbija	96	67	55	12	36	15
Španjolska	88	51	29	22	19	17
Švedska	91	65	66	46	37	21
Turska	76	69	35	7	23	29
MAX	98	75	66	71	43	44
MIN	62	32	15	4	7	11

Izvor: Eurostat ([isoc_cisce_ra](#)) and ([isoc_cisce_ic](#)), ICT security in enterprises, EU, 2022 (% enterprises);

Podaci u Tablici 1. prikazani su za 2022. godinu osim indikatora „Nastali IKT sigurnosni incidenti imali su posljedice“ koji je iskazan za 2021. godinu.

Prema navedenim indikatorima samo tri zemlje su iznad europskog prosjeka u svim kategorijama – Danska, Finska i Malta (od 32 zemlje s popisa). Nizozemska je iznad prosjeka prema 5 parametara i ispod europskog prosjeka je po postotku poslovnih subjekata koji rade na podizanju svijesti zaposlenika o njihovoj odgovornosti vezano uz kibernetičku sigurnost (46%, a EU prosjek iznosi 58%).

Hrvatska spada u skupinu zemalja koje imaju po 2 indikatora iznad prosjeka (od 6 odabranih). U tu kategoriju spadaju još Austrija, Češka, Estonija, Latvija, Slovenija i Turska.

Šest zemalja nema niti jedan parametar iznad prosjeka (Bosna i Hercegovina, Bugarska, Cipar, Grčka, Mađarska, Španjolska).

Prvi pokazatelj govori da postoje poslovni subjekti u zemljama EU koji uopće ne koriste mjere IKT sigurnosti. Tako primjerice na nivou EU 8% poslovnih subjekata ne koristi niti jednu mjeru zaštite od kibernetičkih incidenata. Finska i Danska imaju 98% poslovnih subjekata koji koriste barem jednu mjeru zaštite, što govori da tek 2% ispitanih poslovnih subjekata nije uvelo mjere zaštite. Najkritičnije stanje je u Grčkoj gdje čak četvrtina ispitanih poslovnih subjekata ne koristi uopće mjere IKT sigurnosti.

Kada je riječ o broju poslovnih subjekata koji rade na podizanju razine svijesti zaposlenih oko njihovih obaveza u osiguranju IKT sigurnosti Grčka, kao i u prethodnom slučaju, ima najniži postotak (32%). EU prosjek iznosi 58%. Prema vrijednostima za taj indikator poslovni subjekti u Hrvatskoj (38%) bi također trebali intenzivnije raditi na mjerama za poduzimanje razine svijesti o važnosti kibernetičke sigurnosti te o obvezama i odgovornostima pojedinaca u poslovnom okruženju.

Ispitani poslovni subjekti imaju dokumente o mjerama, praksi i procedurama za IKT sigurnost prosječno u 37% slučajeva na nivou EU. Stanje u Hrvatskoj značajno je bolje od europskog prosjeka, pa se tako čak 49% ispitanih poslovnih subjekata izjasnilo da ima dokumentirane mjere, praksu i procedure za IKT sigurnost.

Interesantan je podatak vezan uz ugovaranje polica osiguranja od šteta nastalih zbog kibernetičkih incidenata. Prema Eurostatu, u 2022. godini, Danska je daleko ispred ostalih. Čak 71% poduzeća ispitanih u istraživanju odgovorilo je da ima ugovorenu policu osiguranja od štete koju mogu imati kibernetički (IKT incidenti). Značajan postotak poslovnih subjekata koji ugovaraju police osiguranja evidentiran je u Švedskoj (46%), Irskoj (42%), Francuskoj (40%), Norveškoj (38%), Malti (35%), Belgiji i Finskoj (33%), Njemačkoj 32%, Luksemburgu (31%), Nizozemskoj (30%) i Austriji (27%). Prema navedenom popisu može se zaključiti da je riječ uglavnom o gospodarski razvijenim zemljama u kojima je digitalizacija poslovanja na razini iznad europskog prosjeka te je stoga mogućnost pojave šteta od kibernetičkih incidenata znatno veća (i po pojavnosti i po utjecaju) u odnosu na ostatak zemalja koje tek intenzivno rade na razvoju digitalnog tržišta. Navedeno govori o razvijenoj svijesti o razmjerima štete koju mogu prouzročiti kibernetički incidenti na kontinuitet poslovanja i reputaciju poslovnog subjekta. U Hrvatskoj tek se 7% poslovnih subjekata izjasnilo da ima ugovorenu policu osiguranja od štete nastale kibernetičkim incidentom.

Dokumentacija vezana uz IKT sigurnost izrađena je ili ažurirana je u posljednjih 12 mjeseci prosječno kod 24% poslovnih subjekata na nivou EU, dok u Hrvatskoj taj podatak iznosi 29%. Najviši postotak evidentiran je u Finskoj, čak 43%, a najniži u Grčkoj i iznosi 7%.

Podatak o postojanju posljedica nakon kibernetičkih incidenata može ukazivati na činjenicu da kod visoko razvijenih zemalja gdje je digitalizacija na visokoj razini (Finska, 44%) postotak poslovnih subjekata može biti veći. Iznad prosjeka po tom indikatoru su još Belgija s 23%, Danska, Estonija, Malta i Njemačka s 26%, Češka s 29% te Nizozemska i Poljska s 30%.

3. ZAKLJUČAK

U članku je prezentiran tek mali dio odabranih pokazatelja koji su vezani uz kibernetičku sigurnost, mjere koje se statistički prate putem nadležne ustanove za statistička istraživanja u EU – Eurostata. Kratki prikaz podataka govori u prilog činjenici da je kibernetička sigurnost trenutno jedan od većih izazova ako se uzme u obzir strateško usmjerenje da se Europa odlučila za održivi rast i razvoj ulaganjem u zeleno i digitalno.

Kibernetička sigurnost podrazumijeva zaštitu imovine (svega što je povezano s IKT), a kako bi globalno mogli govoriti o kibernetički sigurnom poslovnom okruženju, svaki poslovni subjekt dužan je provoditi sve potrebne mjere koje osiguravaju neometan promet i poslovanje u digitalnom okruženju. Da bi u tome na nivou EU uspjeli potrebno je provoditi u praksu usvojenu regulativu i provedbene akte, prije svega na nacionalnoj razini, a onda i niže na razini svakog poslovnog subjekta koji djeluje u digitalnom poslovnom okruženju.

Članak je namijenjen onima koji će u skoro vrijeme biti u prilici posvetiti se intenzivno operativnom provođenju usklade poslovanja s Direktivom NIS 2, a komentirane postojeće vrijednosti odabranih pokazatelja i ideje (npr. police osiguranja) mogu biti poticaj i inspiracija za unapređenje stanja.

REFERENCE

1. Europska Komisija, (2016), DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, preuzeto <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1692602453659>, pristupljeno 10. svibnja 2024.
2. Europska Komisija, (2022), DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), preuzeto <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>, pristupljeno 10. svibnja 2024.
3. Eurostat (2024), ICT security in enterprises, *Data from December 2022*, preuzeto s [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_measures_\(isoc_cisce_ra\)_and_\(isoc_cisce_ic\)](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_measures_(isoc_cisce_ra)_and_(isoc_cisce_ic)), pristupljeno 6. kolovoza 2024.

O autorici

Doc. dr. sc. Robertina Zdjelar doktorirala je u području društvenih znanosti, polje informacijske i komunikacijske znanosti 2022. godine. Tijekom 2024. godine autorica je izabrana u znanstveno-nastavno zvanje naslovni docent. Bavi se istraživanjem u području informacijskih i komunikacijskih znanosti, stručnim radovima u području javnih politika, financija i računovodstva. Angažirana je kao vanjski suradnik na Sveučilištu u Zagrebu na Fakultetu organizacije i informatike Varaždin te na Pravnom fakultetu u Zagrebu te na Geotehničkom fakultetu u Varaždinu. Djelovanje na Fakultetu organizacije i informatike odnosi se na upravljanje kvalitetom u informatici, kvalitetu i mjerenja u informatici, upravljanje primjenom informacijske tehnologije u poslovanju, odgovornost, inkluzija i održivost u informatici. Na Pravom fakultetu u Zagrebu autorica je održala nekoliko predavanja na temu upravljanja projektima. Na Geotehničkom fakultetu u Varaždinu održala je tribinu pod naslovom "Umjetna inteligencija i gospodarenje otpadom".

U poslovnom okruženju autorica je zaposlenik Gradskog komunalnog poduzeća Komunalac d.o.o. kao direktorica Sektora financija, računovodstva i EU projekata, a u okviru kojega se nalaze i druge poslovne funkcije važne za poslovanje društva. Zadnjih osam godina zaposlena je u društvu Komunalac, čemu je prethodilo dvadesetgodišnje radno iskustvo u Koprivničko-križevačkoj županiji na raznim pozicijama, od pripravnika, suradnika do pročelnice za financije, proračun i javnu nabavu.

Autorica posjeduje brojne stručne certifikate od kojih treba istaknuti ISO 27001 interni auditor, ISO 9001 interni auditor, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata. U postupku je stjecanja certifikata za vodećeg implementera NIS 2 direktive. Svoje radno iskustvo koristi kao izvor ideja za znanstvene i stručne radove.