Smjernice za nadležna tijela

o nacionalnoj procjeni kibernetičkih sigurnosnih rizika


NCSC
HR

Sadržaj

I. Pravila definirana člancima 35. do 40. i člankom 42. Uredbe o kibernetičkoj sigurnosti (u daljnjem tekstu: Uredba)

(1) Nacionalna procjena kibernetičkih sigurnosnih rizika (u daljnjem tekstu: nacionalna procjena rizika), provodi se u okviru postupka kategorizacije subjekata za svaki subjekt kategoriziran kao ključan odnosno važan subjekt. Cilj provođenja nacionalne procjene rizika je definirati razinu mjera upravljanja kibernetičkim sigurnosnim rizicima koju je subjekt dužan provoditi.

(2) Nacionalna procjena rizika provodi se na temelju podataka o:

a) veličini subjekta koji se kategorizira (mali, srednji ili veliki temeljem EU kriterija veličine) i

b) pripadnosti subjekta koji se kategorizira u određenom sektoru iz priloga I. i priloga II. Zakona o kibernetičkoj sigurnosti (u daljem tekstu: Zakon).

(3) Na temelju praćenja stanja kibernetičke sigurnosti na globalnoj, EU i nacionalnoj razini te provođenja povezanih sigurnosnih procjena, uvode se sljedeći elementi metodologije koja se koristi:

a) odabir tipičnih vrsta kibernetičkih napada koji se uzimaju kao relevantni za ovu procjenu rizika: poremećaj poslovanja ili sabotaža, krađa podataka ili špijunaža, kibernetički kriminal (npr. *Ransomware*, financijske prijevare), vandalizam sadržaja i dostupnosti podataka na Internetu, politički utjecaj i dezinformacije

b) procjena je li pojedina vrsta tipičnih kibernetičkih napada općenito moguća u nekom sektoru kroz oportunističke napade ili se procjenjuje kao tipična i ciljana vrsta napada za pojedini sektor

c) procjena razine ozbiljnosti poremećaja u funkcioniranju usluga odnosno obavljanju djelatnosti koje odabrane vrste tipičnih kibernetičkih napada mogu uzrokovati u pojedinom sektoru prema globalno raspoloživim podacima

d) odabir tipičnih vrsta kibernetičkih napadača koji se uzimaju kao relevantni za ovu procjenu: državno-sponzorirane APT grupe, teroristi, kibernetičke kriminalne grupe, haktivističke grupe, konkurentski poslovni napadači, zajedno s procjenom tipične razine kibernetičkih vještina odabranih vrsta kibernetičkih napadača

e) procjena vjerojatnosti pojave pojedine vrste kibernetičkih napada, koju uzrokuje određena vrsta kibernetičkih napadača, i to za svaki pojedini sektor te za svaku od odabranih i tipičnih vrsta kibernetičkih napada.

(4) Potrebnu razradu podataka i procjene iz točke 3., za potrebu provedbe nacionalne procjene rizika u sektorima iz Priloga I. i Priloga II. Zakona, provodi središnje državno tijelo za kibernetičku sigurnost, u suradnji s drugim nadležnim tijelima za provedbu kategorizacije subjekata.

(5) Nacionalnu procjenu rizika za svaki pojedini subjekt koji se kategorizira, provode nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti u okviru inicijalnog postupka kategorizacije

subjekta na temelju podataka i procjena iz točke 3., nakon svakog ažuriranja popisa ključnih i važnih subjekata sukladno članku 17. stavku 2. Zakona, te općenito prilikom svake kategorizacije nekog subjekta iz svoje nadležnosti. Pri tome su potrebni ulazni podaci iz točke 2., i to veličina pojedinog subjekta i sektor iz Priloga I. ili Priloga II. Zakona u okviru kojeg se subjekt kategorizira, a svi ostali podaci i procjene osiguravaju se kroz postupak iz točke 4.

(6) Cilj nacionalne procjene rizika je utvrđivanje niske, srednje ili visoke razine kibernetičkih sigurnosnih rizika za svaki pojedini subjekt iz određenog sektora koji se kategorizira temeljem Zakona.

(7) Za svaki subjekt kategoriziran kao ključan ili važan u nekom sektoru iz Priloga I. i Priloga II. Zakona, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti, temeljem utvrđene razine rizika prema točki 5., određuje obvezu provedbe jedne od tri razine mjera upravljanja kibernetičkim sigurnosnim rizicima za taj subjekt, na sljedeći način:

a) za nisku razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom se subjekt obvezuje na provedbu osnovne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. Uredbe

b) za srednju razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom se subjekt obvezuje na provedbu srednje razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. Uredbe

c) za visoku razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom se subjekt obvezuje na provedbu napredne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz Priloga II. Uredbe.

(8) Osnovna razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz točke 7.a. predstavlja opći skup mjera kibernetičke sigurnosti koji je moguće postići s lako dostupnim tehnologijama i dobro poznatim i dokumentiranim najboljim kibernetičkim sigurnosnim praksama, primjeren u slučaju manjih subjekata ili subjekata čije djelatnosti pripadaju sektorima za koje nisu tipični ciljani kibernetički napadi koje provode napadači s višom razinom kibernetičkih vještina, a cilj primjene osnovne razine je zaštiti subjekt od većine globalno prisutnih kibernetičkih napada, odnosno od kibernetičkih napada koje provode kibernetički napadači prosječnih kibernetičkih vještina.

(9) Srednja razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz točke 7.b. predstavlja dopunjeni skup mjera kibernetičke sigurnosne prakse kojim se nadograđuje osnovna razina mjera upravljanja kibernetičkim sigurnosnim rizicima opisana u točki 8., a cilj primjene srednje razine je dodatno umanjiti rizike od ciljanih kibernetičkih napada koje provode kibernetički napadači prosječnih kibernetičkih vještina.

(10) Napredna razina mjera upravljanja kibernetičkim sigurnosnim rizicima iz točke 7.c. predstavlja dopunjeni skup mjera kibernetičke sigurnosne prakse kojim se nadograđuje srednja razina mjera upravljanja kibernetičkim sigurnosnim rizicima opisana u točki 9., a cilj primjene

napredne razine je smanjenje rizika od naprednih kibernetičkih napada koje provode kibernetički napadači s naprednim vještinama i resursima.

(11) U slučajevima kada subjekt pruža usluge ili obavlja djelatnosti koje pripadaju u više različitih sektora iz Priloga I. i Priloga II. Zakona, nacionalna procjena rizika se provodi za glavnu djelatnost subjekta. Ukoliko se glavna djelatnost subjekta ne može nedvojbeno utvrditi, nacionalna procjena rizika provodi se za sve usluge i djelatnosti zbog kojih je subjekt kategoriziran kao ključan ili važan subjekt te se kao konačna nacionalna procjena rizika subjekta uzima najviša utvrđena razina kibernetičkih sigurnosnih rizika prema točki 7.

II. Metodologija za provedbu nacionalne procjene rizika

(12) Nacionalna procjena rizika, kao i utvrđivanje obvezujuće razine mjera upravljanja kibernetičkim sigurnosnim rizicima za ključne i važne subjekte prema točki 7., provodi se sukladno ovim Smjernicama za nacionalnu procjenu kibernetičkih sigurnosnih rizika, s ciljem ujednačavanja pristupa u ovom postupku u svim nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti na nacionalnoj razini. U cilju jednostavnijeg i bržeg postupanja, središnje državno tijelo za kibernetičku sigurnost izrađuje i periodično ažurira tablični kalkulator za izračun razine kibernetičkih sigurnosnih rizika prema podacima i procjenama iz točke 3., pri čemu se u procjeni koriste sva raspoloživa iskustva na globalnoj i nacionalnoj razini kibernetičke sigurnosti.

(13) Smjernice se donose u svrhu izrade metodologije kojom će se sistematizirati i unificirati potrebni podaci i procjene postavljene zahtjevima iz točke 3. te razraditi prikladni tablični kalkulator za izračun razine nacionalne procjene rizika za pojedine subjekte, a koji će koristiti nadležna tijela za provedbu zahtjeva kibernetičke sigurnosti u okviru postupka kategorizacije svakog pojedinog subjekta. Na taj način će se za svaki subjekt, sukladno njegovoj veličini i pripadnosti određenom sektoru iz Priloga I. ili Priloga II. Zakona, odrediti njegova nacionalna razina rizika (niska, srednja, visoka), koja će se prema točki 7. povezati s jednim od skupova mjera kibernetičke sigurnosti (osnovna, srednja, napredna) iz Priloga II. Uredbe, koji će subjekt biti obvezan provoditi.

(14) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti će u okviru kategorizacije svakog pojedinog subjekta iz svoje nadležnosti, dati subjektu uputu o obvezujućem korištenju jednog od skupova mjera koji proizlazi temeljem nacionalne procjene razine rizika sukladno točki 7.

(15) Veličina subjekta uzima se kao obvezujući kriterij u okviru nacionalne procjene rizika. Pri tome se za velike, srednje i male subjekte koriste kvantificirane vrijednosti: veliki = 3, srednji = 2 i mali = 1.

(16) Pripadnost subjekta određenom sektoru iz Priloga I. i Priloga II. Zakona uzima se kao obvezujući kriterij za nacionalnu procjenu rizika. Pri tome se ova obaveza ne primjenjuje za sektore u kojima se koristi posebna sektorska regulativa u okviru koje su propisane odgovarajuće mjere kibernetičke sigurnosti koje su više od zahtjeva utvrđenih Zakonom o kibernetičkoj sigurnosti.

(17) Za procjenu nacionalnih kibernetičkih rizika koriste se tipične i unaprijed određene kategorije kibernetičkih napada:

1. poremećaj poslovanja/sabotaža,

2. krađa podataka/špijunaža,

3. kibernetički kriminal (npr. *Ransomware*, financijske prijevare),

4. vandalizam sadržaja i dostupnosti podataka na Internetu (npr. *defacing*, DDOS) te

5. politički utjecaj i dezinformacije.

(18) Pet kategorija kibernetičkih napada iz točke 17., procjenjuju se za svaki pojedini sektor iz Zakona u smislu globalne i/ili nacionalne prisutnosti ovih vrsta napada u pojedinim sektorima. Pri tome se ove vrste kibernetičkih napada za svaki pojedini sektor procjenjuju kao opći (mogu zahvatiti sektor kroz oportunističke napade, kvantificirana vrijednost = 1) ili ciljani (direktno usmjereni napadi na pojedini sektor, kvantificirana vrijednost = 2).

(19) Pet kategorija kibernetičkih napada iz točke 17., za svaki pojedini sektor Zakona, procjenjuju se i u smislu utjecaja koji takve vrste kibernetičkih napada tipično mogu uzrokovati u pojedinom sektoru i to na tri razine: visoka, srednja i niska, koje se kvantificiraju kao: visoka = 10, srednja = 5 i niska = 0.

(20) Vrste kibernetičkih napadača se za potrebe ovih smjernica kategoriziraju na sljedeći način te im se pri tome pridružuju tipične razine vještina (prosječne, proširene, napredne):

1. konkurentski napadači (poslovni aspekt) – prosječne vještine

2. haktivisti (ideološki) – prosječne vještine

3. teroristi – proširene vještine

4. kibernetički kriminalci – proširene vještine

5. državno-sponzorirani napadači (APT grupe) – napredne vještine

(21) Za svaku od pet kategorija kibernetičkih napada iz točke 17. i za svaku od pet vrsta kibernetičkih napadača iz točke 20., procjenjuje se vjerojatnost događanja pojedine vrste napada koju uzrokuje određena vrsta kibernetičkog napadača za svaki pojedini sektor iz Priloga I. i Priloga II. Zakona. Vjerojatnost se procjenjuje kao visoka, srednja i niska, te se kvantificira kao: visoka = 1, srednja = 0,5 i niska = 0. Pri tome se u slučaju niske razine vjerojatnosti procjenjuje da određena vrsta napadača nije bila prisutna u određenom sektoru (globalno i/ili lokalno) te da se to niti ne očekuje u bližoj budućnosti. To znači da je je rizik od takve vrste napadača prihvatljiv i da nije potrebno primjenjivati dodatne mjere. U slučaju srednje razine vjerojatnosti, procjenjuje se da postoje zabilježeni napadi ove vrste koje provode određene vrste napadača u pojedinom sektoru (globalno i/ili lokalno) te postoji srednja razina vjerojatnosti njihove nacionalne pojave i to u bližoj budućnosti. Takav rizik je prihvatljiv uz primjenu određenih dodatnih mjera. U slučaju visoke razine vjerojatnosti, procjenjuje se kako pojedine vrste napadača provode neke vrste napada uobičajeno u određenom sektoru te se pojava tih napada očekuje i u nacionalnom okruženju u bližoj budućnosti. Takav rizik je neprihvatljiv i mora se svesti na najmanju moguću mjeru primjenom određenih dodatnih mjera.

(22) Izračun razine nacionalnog rizika provodi se na temelju uvedenih kvantificiranih veličina u prethodnim točkama, uzimajući u obzir sektore iz Priloga I. i Priloga II. Zakona, kao i kategorije vrsta napada i vrsta napadača koje su uvedene ovim Smjernicama te određujući globalna ili ciljana obilježja pojedinih napada za određeni sektor, kao i vjerojatnost kombinacija pojedinih vrsta kibernetičkih napada i kibernetičkih napadača za svaki pojedini sektor.

(23) Parametri iz točaka 18., 19. i 21. (kvantificirane veličine za vjerojatnosti, procjene i utjecaj) koriste se na sljedeći način u cilju izračuna ukupnog rezultata za kvantificiranu razinu rizika za svakog pojedinog subjekta za kojeg nadležno tijelo posjeduje podatke iz točke 2. (veličina subjekta i pripadnost nekom sektoru Zakona):

1. temeljem veličine subjekta odrediti njegovu kvantificiranu vrijednost veličine (3, 2 ili 1)

2. prema sektoru poslovanja subjekta odabrati kvantificirane procjene iz točke 21. za ovaj sektor ili više njih sukladno točki 11.

3. za svaku kategoriju napada koristiti podatke o prisutnosti te kategorije napada na globalnoj razini nekog sektora ili o ciljanom djelovanju takvih napada na subjekte iz tog sektora i kvantificirati ih kao 1 ili 2

4. za svaku vrstu napadača pomnožiti kvantificiranu veličinu subjekta s procijenjenim faktorom globalnog ili ciljanog napada, zatim to pomnožiti s procijenjenom razinom utjecaja vrste kibernetičkog napada (kvantificirane veličine 10, 5 ili 0) i na kraju sve to još pomnožiti s procijenjenom razinom vjerojatnosti događanja takvog napada koji provodi određena vrsta napadača u odabranom sektoru (kvantificirana vrijednost 1, 0.5 ili 0)

5. pojedinačne iznose rizika koji se prema podtočki 4. dobiju za svaku pojedinu vrstu napadača i za vjerojatnost njegove provedbe svake od tipičnih vrsta kibernetičkih napada u odabranom sektoru, potrebno je zbrojiti u cilju dobivanja ukupne kvantificirane razine nacionalnog rizika za pojedini subjekt u određenom sektoru.

(24) Kvantificirane razine nacionalnog rizika, izračunate prema točki 23., koriste se za izbor osnovne, srednje ili napredne razine obvezujućih mjera i to na sljedeći način:

1. za kvantificirane razine rizika za koje je rezultat između 0 i 99, obvezujuća je osnovna razina mjera

2. za kvantificirane razine rizika za koje je rezultat između 100 i 199, obvezujuća je srednja razina mjera

3. za kvantificirane razine rizika za koje je rezultat 200 i više, obvezujuća je napredna razina mjera.

(25) U cilju primjene opisane metodologije na sve subjekte iz svih sektora, potrebno je unaprijed odrediti sve procjene potrebnih kvantificiranih vrijednosti koje se koriste u izračunu kvantificirane razine nacionalnog rizika za pojedine subjekte prema točki 23. Ove procjene provodi središnje državno tijelo za kibernetičku sigurnost, u suradnji s nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti te prema potrebi kroz konzultacije s pojedinim sektorskim subjektima.

(26) U cilju učinkovitosti i konzistentne provedbe nacionalne procjene kibernetičkih sigurnosnih rizika u okviru više nadležnih tijela za provedbu zahtjeva kibernetičke sigurnosti i za veliki

broj subjekata, izračun kvantificirane razine nacionalnog rizika provodi se pomoću automatiziranog tabličnog kalkulatora koji razvija i održava središnje državno tijelo za kibernetičku sigurnost.

(27) Procjene potrebnih kvantificiranih vrijednosti automatiziranog alata usklađuju se prije inicijalne provedbe kategorizacije subjekata prema Zakonu, te za svaku narednu periodičnu kategorizaciju koja se provodi najmanje jednom u dvije godine, odnosno prema potrebi i procjeni nadležnih tijela.

(28) Sektori, podsektori, vrste subjekata iz priloga I. i II. Zakona, niže ispisani s brojčanim oznakama iz Zakona u zagradama, koriste se u okviru sljedećih 15 kategorija u ovoj metodologiji:

1. (I.1.) Energetika

2. (I.2.) Promet

3. (I.5.) Zdravstvo

4. (I.6.) Voda za ljudsku potrošnju

5. (I.7.) Otpadne vode

6. (I.8.) Digitalna infrastruktura (I.9.) i Upravljanje uslugama IKT-a (B2B)

7. (I.10) Javni sektor

8. (I.11.) Svemir

9. (II.1.) Poštanske i kurirske usluge

10. (II.2.) Gospodarenje otpadom

11. (II.3.) Izrada, proizvodnja i distribucija kemikalija

12. (II.4.) Proizvodnja, prerada i distribucija hrane

13. (II.5. od a do f) Proizvodnja

14. (II.6.) Pružatelji digitalnih usluga

15. (II.7.) Istraživanje i (II.8.) Sustav obrazovanja.

III. Procjena parametara zadanih u okviru metodologije za provedbu nacionalne procjene rizika

(29) Za svaku od 15 kategorija u koje su razvrstani sektori iz Priloga I. i Priloga II. Zakona prema točki 28., niže su razrađeni parametri procjene rizika, utjecaja i vjerojatnosti, koji se odnose na procjene za svaku od 15 kategorija i vezano za uvedenih 5 vrsta kibernetičkih napada prema točki 17., odnosno za 5 vrsta kibernetičkih napadača prema točki 20. Cilj metodologije je da nadležna tijela za kategorizaciju unosom dvaju parametara ključnog ili važnog subjekta prema točki 2., njegove veličine (EU kriteriji) i njegove pripadnosti jednoj od 15 kategorija iz točke 28., gdje su razvrstani svi sektori, podsektori, vrste subjekata iz Priloga I. i Priloga II. Zakona, kao rezultat dobiju parametar koji će im prema točki 24., omogućiti određivanje jedne od triju razina mjera kibernetičke sigurnosti: osnovne, srednje ili napredne.

1. (I.1.) Energetika

Vrsta kibernetičkog napada:	**Opća ili ciljana prisut-nost napada:**	**Razina utjecaja napada:**	**Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:**				
			Konku-rentski napadači:	**Haktivisti:**	**Teroristi:**	**Kibernetički kriminalci:**	**Državno-sponzorirani napadači (APT grupe):**
Poremećaj poslovanja /sabotaža	2	10	0	0	0,5	0,5	1
Krađa podataka /špijunaža	2	10	0	0	0	1	1
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0,5
Politički utjecaj i dezinformacije	1	0	0	0,5	0	0	0

2. (I.2.) Promet

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0	0,5	0	1
Krađa podataka /špijunaža	2	10	0	0	0	1	1
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0,5
Politički utjecaj i dezinformacije	1	1	0	0,5	0	0	0

3. (I.5.) Zdravstvo

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	0,5	0	0,5
Krađa podataka /špijunaža	2	10	0	0	0,5	0,5	0,5
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	0	0	0	0	0	0
Politički utjecaj i dezinformacije	1	5	0	0,5	0	0	0

4. (I.6.) Voda za ljudsku potrošnju

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	1	0	1
Krađa podataka /špijunaža	2	5	0	0	0,5	0,5	0,5
Kibernetički kriminal	1	5	0	0	0	0,5	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	0	0	0	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0	0	0	0

5. (I.7.) Otpadne vode

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	1	0	1
Krađa podataka /špijunaža	2	5	0	0	0,5	0,5	0,5
Kibernetički kriminal	1	5	0	0	0	0,5	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	0	0	0	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0	0	0	0

6. (I.8.) Digitalna infrastruktura i (I.9.) Upravljanje uslugama IKT-a (B2B)

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	0,5	0	1
Krađa podataka /špijunaža	2	10	0	0	0	1	1
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0,5
Politički utjecaj i dezinformacije	1	0	0	0,5	0,5	0	0

7. (I.10) Javni sektor

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	0,5	0,5	1
Krađa podataka /špijunaža	2	10	0	0	0,5	1	1
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	10	0	0,5	0	0	0,5
Politički utjecaj i dezinformacije	1	10	0	0,5	0	0	0

8. (I.11.) Svemir

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0	0,5	0	1
Krađa podataka /špijunaža	2	10	0	0	0	1	1
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0,5
Politički utjecaj i dezinformacije	1	5	0	0,5	0	0	0

9. (II.1.) Poštanske i kurirske usluge

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	0,5	0,5	0,5
Krađa podataka /špijunaža	2	5	0	0	0	0	0,5
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	0	0	0	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0,5	0	0	0

10. (II.2.) Gospodarenje otpadom

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	5	0	0	0,5	0	0,5
Krađa podataka /špijunaža	2	0	0	0,5	0,5	0,5	0,5
Kibernetički kriminal	1	5	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0,5	0	0	0

11. (II.3.) Izrada, proizvodnja i distribucija kemikalija

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0	0,5	0	1
Krađa podataka /špijunaža	2	5	0	0,5	0,5	0,5	0,5
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0,5	0	0	0

12. (II.4.) Proizvodnja, prerada i distribucija hrane

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0	0,5	0	1
Krađa podataka /špijunaža	2	0	0	0	0	0	0,5
Kibernetički kriminal	1	10	0	0	0	0,5	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0,5
Politički utjecaj i dezinformacije	1	5	0	0,5	0	0	0

13. (II.5. od a do f) Proizvodnja

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	5	0,5	0	0	0	0,5
Krađa podataka /špijunaža	2	10	1	0	0	0,5	0,5
Kibernetički kriminal	1	5	0	0	0	1	0,5
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	0	0	0,5	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0	0	0	0

14. (II.6.) Pružatelji digitalnih usluga

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	10	0	0,5	0,5	0	0,5
Krađa podataka /špijunaža	2	5	0	0,5	0	0,5	0,5
Kibernetički kriminal	1	5	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	0	0	0	0	0	0
Politički utjecaj i dezinformacije	1	5	0	0,5	0	0	0,5

15. (II.7.) Istraživanje i (II.8.) Sustav obrazovanja

Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
Poremećaj poslovanja /sabotaža	2	5	0	0	0	0	0
Krađa podataka /špijunaža	2	10	0,5	0	0,5	0,5	1
Kibernetički kriminal	1	10	0	0	0	1	0
Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0
Politički utjecaj i dezinformacije	1	0	0	0	0	0	0,5

(30) Formula za računanje razine rizika s primjerom tablice:

(I.1.) Energetika

A	B	C	Vrsta kibernetičkih napadača i vjerojatnost njihove provedbe pojedine vrste napada:				
			D	E	F	G	H
Vrsta kibernetičkog napada:	Opća ili ciljana prisut-nost napada:	Razina utjecaja napada:	Konku-rentski napadači:	Haktivisti:	Teroristi:	Kibernetički kriminalci:	Državno-sponzorirani napadači (APT grupe):
1 Poremećaj poslovanja /sabotaža	2	10	0	0	0,5	0,5	1
2 Krađa podataka /špijunaža	2	10	0	0	0	1	1
3 Kibernetički kriminal	1	10	0	0	0	1	0
4 Vandalizam sadržaja i dostupnosti podataka na Internetu	1	5	0	0,5	0	0	0,5
5 Politički utjecaj i dezinformacije	1	0	0	0,5	0	0	0

Formula:

D = {[(D1 x C1 x B1) x VELIČINA] + [(D2 x C2 x B2) x VELIČINA] + [(D3 x C3 x B3) x VELIČINA] + [(D4 x C4 x B4) x VELIČINA] + [(D5 x C5 x B5) x VELIČINA]}

Napomena: VELIČINA je veličina tvrtke prema EU kriterijima kvantificirana prema točki 15., a D je rezultirajuća razina rizika za stupac D (konkurentski napadači)

Formulu je potrebno adekvatno primijeniti za stupce E, F, G i H (razine rizika za svaku pojedinu vrstu napadača).

Ukupan rezultat jednak je zbroju razina rizika za svih pet stupaca, odnosno vrsta napadača: D+E+F+G+H

Rezultat je potrebno usporediti s razinama definiranim prema točki 24., a prema potrebi se primjenjuje postupak iz točke 11.

Prilog:

Kalkulator za izračun razine rizika po sektorima iz točke 28. Smjernica

(Excel datoteka „KalkulatorRizika_28022025[1]“)

[1] https://ncsc.hr/UserDocsImages/kategorizacija/KalkulatorRizika_28022025.xlsx

Sigurnosno-obavještajna agencija

Nacionalni centar za kibernetičku sigurnost

Savska cesta 39/1, 10000 Zagreb

Republika Hrvatska

KONTAKT:

E-mail: info@ncsc.hr

www.ncsc.hr