Smjernice za kategorizirane subjekte

o upravljanju kibernetičkim sigurnosnim rizicima


NCSC
HR

Sadržaj

I. Uvod 1
II. Zahtjevi strukturiranog procesa upravljanja kibernetičkim sigurnosnim rizicima 2
III. Proces upravljanja rizikom kibernetičke sigurnosti 3
IV. Vlasnik rizika 5
V. Ključni pojmovi 7
VI. Pristupi, metode i tehnike koje se koriste u procjeni rizika 10
VII. PRILOG – Primjeri tipičnih prijetnji i ranjivosti 12

I. Uvod

Zakonom o kibernetičkoj sigurnosti („Narodne novine“, broj 14/24., u daljnjem tekstu: ZKS) te Uredbom o kibernetičkoj sigurnosti („Narodne novine“, broj 135/24., u daljnjem tekstu: Uredba) postavljeni su zahtjevi za provedbu upravljanja kibernetičkim sigurnosnim rizicima (članak 45. stavak 3. Uredbe i mjera 3. Priloga II. Uredbe).

Subjekti ZKS-a mogu za upravljanje kibernetičkim sigurnosnim rizicima, pored ovih Smjernica, koristiti relevantne međunarodne i EU norme te najbolje prakse koje zadovoljavaju zahtjeve postavljene Uredbom.

Osobe odgovorne za upravljanje kibernetičkim sigurnosnim rizicima su članovi upravljačkih tijela ključnih i važnih subjekata odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršnih tijela jedinica lokalne i područne (regionalne) samouprave.

Subjekt ZKS-a koji ima uspostavljene procese upravljanja rizicima na razini poslovanja subjekta provodi upravljanje rizikom opisano u okviru podskupova mjere 3. Priloga II. Uredbe (3.1. do. 3.7.) integrirano, kao dio prije uspostavljenog procesa upravljanja rizicima poslovanja subjekta. Ako subjekt nema uspostavljene procedure upravljanja rizicima na razini poslovanja subjekta, uspostavlja mjeru 3. Priloga II. Uredbe (3.1. do 3.7.) kao novi poslovni proces. U tom slučaju, kada subjekt ZKS-a uspostavlja novi poslovni proces upravljanja rizicima kibernetičke sigurnosti, preporuča se da tijekom roka od prvih 12 mjeseci za provedbu obvezujućih mjera iz razine određene kategorizacijom (osnovna, srednja ili napredna), prvo provede sve obvezujuće mjere osim mjere 3. Priloga II. Uredbe. Nakon toga se preporuča da tijekom narednih 12 mjeseci uvede novi poslovni proces upravljanja rizicima kibernetičke sigurnosti sukladno zahtjevima iz mjere 3. Priloga II. Uredbe, kroz koji će dodatno postaviti prioritete i opseg pojedinih mjera provedenih tijekom prvih 12 mjeseci.

U posljednjoj, trećoj godini od kategorizacije subjekta, subjekti moraju provesti samoprocjenu (važni subjekti) ili reviziju (ključni subjekti) kibernetičke sigurnosti, što predstavlja daljnju trajnu i periodičnu obavezu samoprocjena, odnosno revizija tijekom svake naredne dvije godine.

Procjena rizika provodi se sukladno zahtjevima iz članka 48. Uredbe, odnosno najmanje jednom godišnje u okviru redovite godišnje procjene rizika subjekta.

II. Zahtjevi strukturiranog procesa upravljanja kibernetičkim sigurnosnim rizicima

(1) Kibernetički sigurnosni rizici predstavljaju strateške sigurnosne rizike koji mogu utjecati na poslovanje pravne osobe u cjelini. Stoga se preporučuje integracija upravljanja kibernetičkim sigurnosnim rizicima u sustav upravljanja poslovnim rizicima, ukoliko je pravna osoba implementirala sustav upravljanja poslovnim rizicima. Ukoliko pravna osoba nije uspostavila sustav upravljanja poslovnim rizicima, pravna osoba mora uspostaviti proces upravljanja kibernetičkim sigurnosnim rizicima kao novi proces.

(2) Ključni elementi procesa upravljanja kibernetičkim sigurnosnim rizicima sastoje se od načela, okvira i procesa upravljanja.

(3) Ključna načela procesa upravljanja kibernetičkim sigurnosnim rizicima su da taj proces predstavlja integralni dio svih organizacijskih aktivnosti, da je strukturiran i sveobuhvatan, prilagođen i proporcionalan vanjskim i unutarnjim sadržajima povezanim s ciljevima organizacije, inkluzivan u smislu uključenja svih dionika pravne osobe, dinamičan u smislu praćenja nastajanja, promjena ili nestajanja pojedinih rizika, temeljen na najboljim mogućim povijesnim i aktualnim podacima, kao i budućim očekivanjima, uzimajući pri tome u obzir ljudske i kulturološke čimbenike, kao i kontinuirano unaprjeđenje ovog procesa kroz učenje i iskustvo.

(4) Učinkovitost procesa upravljanja kibernetičkim sigurnosnim rizicima ovisi o integraciji upravljanja rizikom s upravljanjem i odlučivanjem kakvo je uspostavljeno u organizaciji. Okviri procesa trebaju biti postavljeni tako da uključuju vodstvo organizacije i njegovu predanost oblikovanju ovog procesa upravljanja rizicima kibernetičke sigurnosti. Proces upravljanja kibernetičkim sigurnosnim rizicima potrebno je implementirati, kontinuirano evaluirati te stalno unaprjeđivati.

(5) Proces upravljanja kibernetičkim sigurnosnim rizicima mora biti trajan proces koji uključuje sustavnu primjenu politika, procedura i praksi kroz aktivnosti komunikacije i savjetovanja sa svim dionicima poslovnih procesa organizacije, u cilju uspostavljanja konteksta za procjenu, obradu, praćenje i ažuriranje rizika za mrežne i informacijske sustave, kao i pohrane povijesnih podataka u ovom periodičnom procesu te izvještavanja o rizicima prema dionicima organizacije odgovornima za poslovne procese.

(6) Rizici kibernetičke sigurnosti predstavljaju strateške rizike svakog subjekta ZKS-a, odnosno rizike čiji utjecaj na subjekt može biti devastirajući zbog visoke razine ovisnosti poslovnih procesa o mrežnim i informacijskim sustavima. Potrebno je primijeniti pristup koji uključuje sve vrste rizika (engl. *All-Hazards Approach*), odnosno pristup u kojem se procjenjuju kvarovi, nesreće i napadi (engl. *Failure, Accidents, Attacks*).

III. Proces upravljanja rizikom kibernetičke sigurnosti

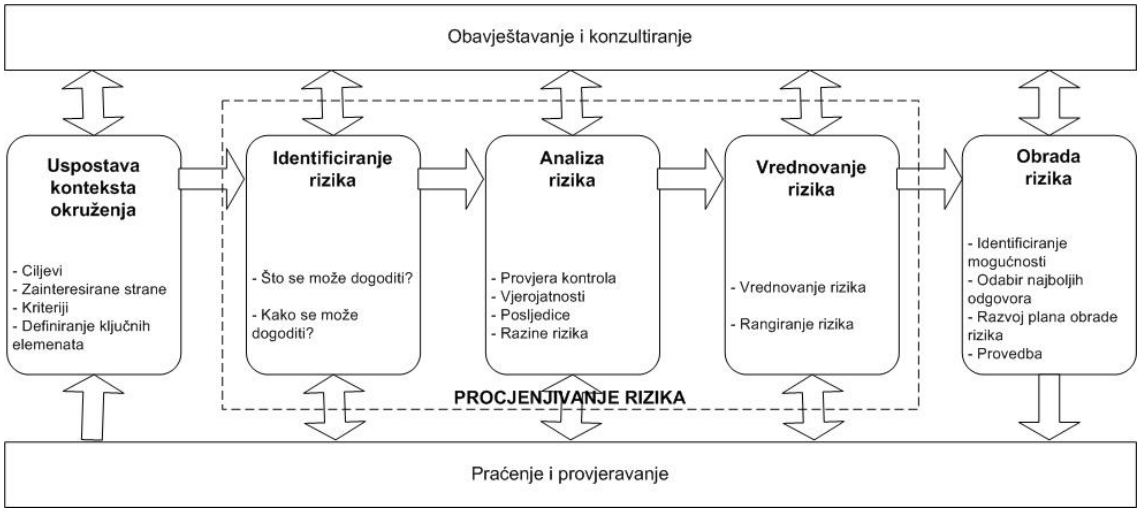
(7) Proces upravljanja rizikom u osnovi se sastoji od sljedećih segmenata koji su prikazani na Slici 1.:

1. uspostava konteksta okruženja subjekta u smislu usklađenog poslovnog opsega i povezanih mrežnih i informacijskih sustava,

2. procjenjivanje rizika (identificiranje, analiza i vrednovanje),

3. obrada rizika (izbjegavanje, modificiranje, prihvaćanje i dijeljenje),

4. uspostava cjeloživotnog procesa upravljanja rizikom kibernetičke sigurnosti (periodično godišnje ažuriranje).



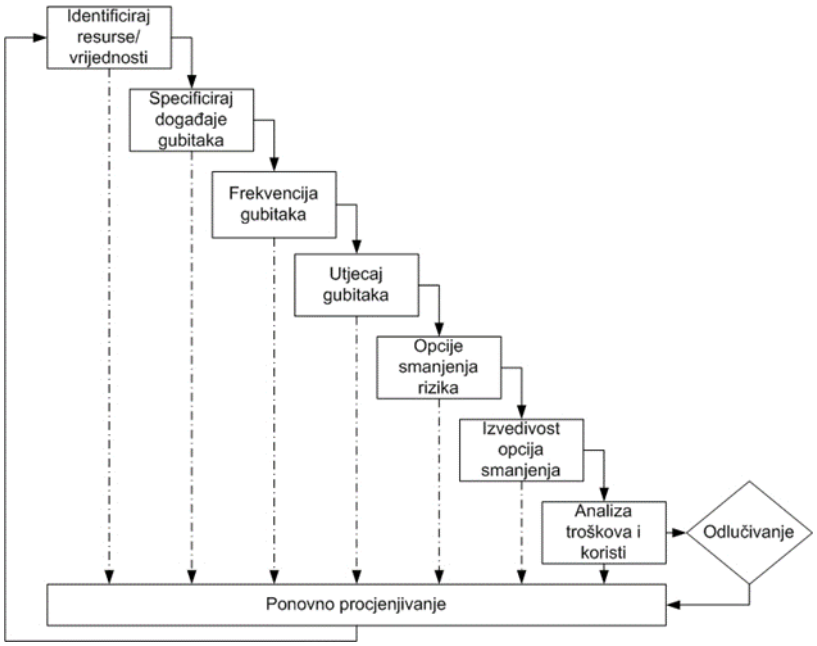
Slika 1. - Segmenti procesa upravljanja rizikom

(8) Uspostava konteksta okruženja subjekta je iznimno važna jer se upravljanje rizikom kibernetičke sigurnosti provodi za cjelokupno poslovanje subjekta, odnosno i za IT i za OT dio mrežnog i informacijskog sustava. Pri tome je potrebno obuhvatiti i sve dijeljene IT infrastrukture poput korištenja računalstva u oblaku, kao i povezanost mrežnog i informacijskog sustava subjekta s drugim mrežnim i informacijskim sustavima, primjerice dobavljača usluga subjekta.

(9) Procjenjivanje rizika treba imati sva tri segmenta prikazana na Slici 1., razrađena u kontekstu subjekta koji provodi procjenjivanje rizika kroz faze identificiranja rizika, analize rizika i vrednovanja rizika.

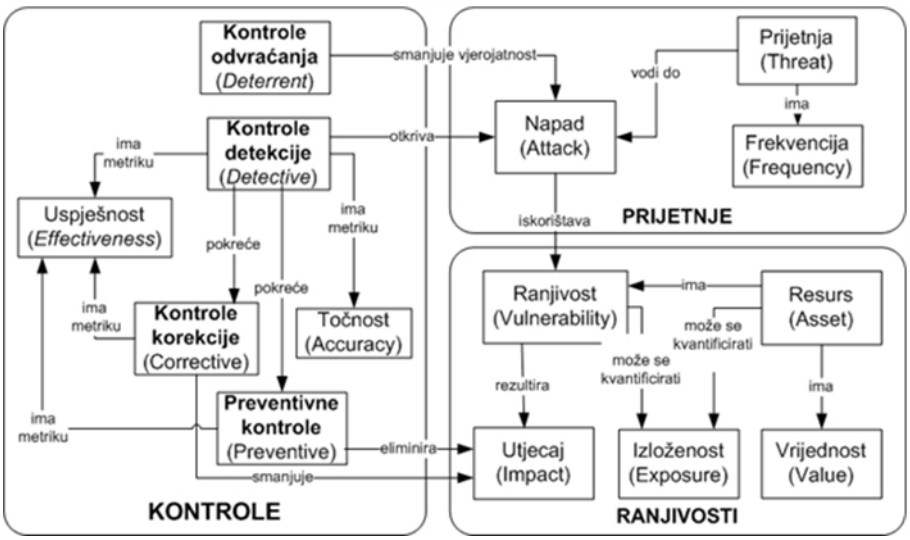
(10) Cilj procjene rizika je priprema za obradu rizika, odnosno njegovo izbjegavanje, modificiranje, prihvaćanje ili dijeljenje. Za prikladnu obradu rizika nužno je razumijevanje rizika u kontekstu samog subjekta koji provodi upravljanje rizikom.

(11) Na Slici 2. prikazan je općeniti periodički proces procjenjivanja sigurnosnog rizika sa svojim glavnim sastavnicama. U osnovi sve norme i najbolje prakse koje uređuju proces upravljanja rizikom prate faze sa Slike 2.



Slika 2. - Općeniti proces procjenjivanja sigurnosnog rizika

(12) Temelj procesa obrade rizika čini implementacija kontrola, koje predstavljaju podskup mjera, odnosno podmjera koje su razrađene u točki 3. Priloga II. Uredbe. Na Slici 3. prikazan je logički model kontrola i njihova podjela na kontrole odvraćanja, detekcije i korekcije te na preventivne kontrole. Cilj uvođenja kontrola je smanjivanje vjerojatnosti rizičnih događaja, njihovo otkrivanje te smanjivanje ili eliminiranje utjecaja rizičnih događaja na okruženje subjekta.

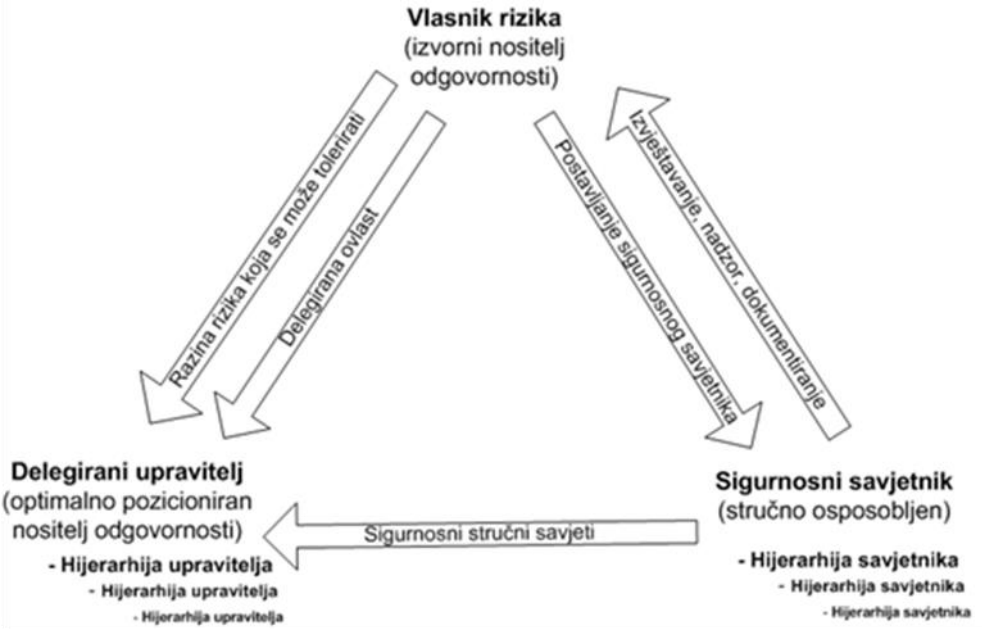


Slika 3. - Logički model sigurnosnih kontrola

IV. Vlasnik rizika

(13) Temeljno načelo upravljanja rizikom je načelo pridruživanja odgovornosti entitetu koji je najbolje pozicioniran za upravljanje rizikom. U subjektima ZKS-a osobe odgovorne za upravljanje kibernetičkim sigurnosnim rizicima su članovi upravljačkih tijela ključnih i važnih subjekata odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršnih tijela jedinica lokalne i područne (regionalne) samouprave.

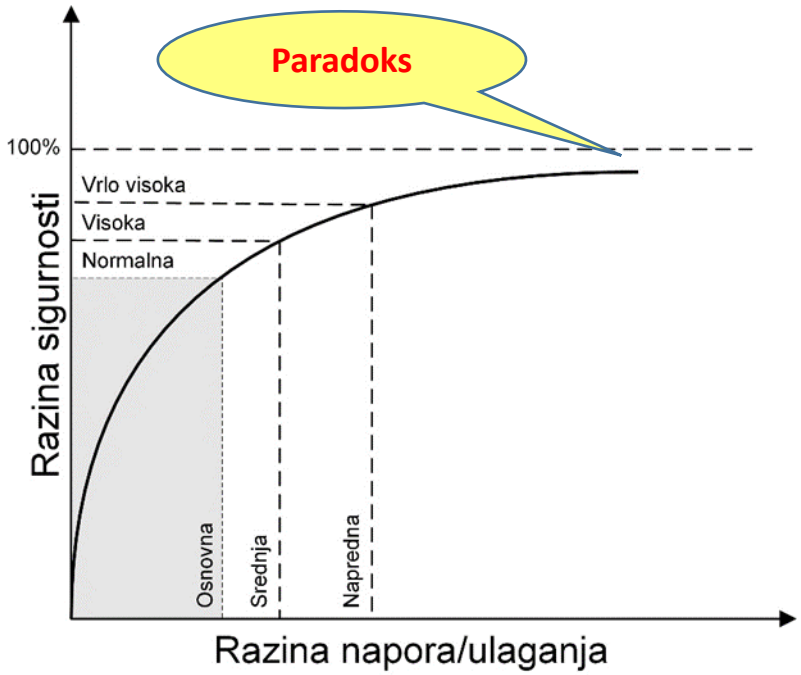
(14) Organizacija upravljanja kibernetičkim sigurnosnim rizicima sastoji se od prepoznavanja vlasnika rizika (izvorni nositelj odgovornosti prema točki 13. ovih Smjernica), delegiranog upravitelja (zainteresirani nositelj) te sigurnosnog savjetnika (stručno osposobljeni savjetnik). Vlasnik rizika određuje opseg primjene, procjenjuje razinu rizika koju može tolerirati (engl. *Risk Apetite*), određuje delegiranog upravitelja te se na odgovarajući način uključuje u provođenje postupka odabira sigurnosnog savjetnika. Delegirani upravitelj provodi upravljanje rizikom u opsegu svoje poslovne nadležnosti i u zadanim granicama tolerancije rizika koju je definirao subjekt, odnosno vlasnik rizika, a pri tome dobiva kompetentne savjete sigurnosnog savjetnika. Opisani trokut međuodnosa vlasnika rizika, delegiranog upravitelja i sigurnosnog savjetnika može se proširivati po horizontali, tako da vlasnik rizika određuje više delegiranih upravitelja za pojedine segmente poslovanja subjekta, odnosno po vertikali u slučaju velikih subjekata, tako da se odredi organizacijska hijerarhija upravljanja kibernetičkim sigurnosnim rizicima kojom upravlja delegirani upravitelj, a paralelno s njom i hijerarhija savjetnika (Slika 4.).



Slika 4. - Princip pridruživanja odgovornosti za upravljanje rizikom u subjektu ZKS-a

(15) Opisani princip pridruživanja odgovornosti za rizik poslovnom entitetu najbolje pozicioniranom za upravljanje rizikom, može se prepoznati i u drugim segmentima politika kibernetičke i informacijske sigurnosti. Primjerice, jedan od čestih slučajeva je da se proces upravljanja rizikom provodi u središnjoj instituciji (državno tijelo ili trgovačko društvo), a decentralizirani organizacijski segmenti (pravne osobe u nadležnosti državnog tijela ili tvrtke kćeri) to provode po potrebi i pod određenim uvjetima, dok redovito moraju provesti skup sigurnosnih

mjera koji definira središnja institucija. U ovom slučaju, prema terminologiji sa Slike 4., radi se o procjeni vlasnika rizika za uspostavu sigurnosnih mjera u decentraliziranoj jedinici. Ta procjena može ići u smjeru procjenjivanja rizika u središnjoj instituciji i primjeni rezultata na lokalne podružnice u obliku definiranog skupa mjera, ili pak može ići u smjeru delegiranja ovlasti za procjenjivanje rizika u lokalnom okruženju i odlučivanju o primjeni sigurnosnih mjera za smanjivanje tako procijenjenih rizika. Na sličan način je i u ZKS-u i Uredbi definirana nacionalna razina procjene rizika koju provodi središnje državno tijelo za kibernetičku sigurnost (NCSC-HR), a kojom se utvrđuje obvezujuća razina mjera za pojedini subjekt (osnovna, srednja ili napredna) prema Slici 5., dok u okviru provedbe ovih obvezujućih mjera kategorizirani subjekt mora uspostaviti i vlastito, lokalno upravljanje rizicima kibernetičke sigurnosti, i temeljem rezultata ovog procesa lokalnog upravljanja rizikom dodatno optimizirati obvezujuće mjere kibernetičke sigurnosti ili prema potrebi provesti i druge dobrovoljne mjere kibernetičke sigurnosti iz Priloga II. Uredbe, označene slovom C.



Slika 5. - Paradoks nepostojanja potpune sigurnosti i njegova pozitivna strana koja omogućava postizanje željene razine sigurnosti uz razumne napore i ulaganja

V. Ključni pojmovi

(16) **Rizik** (engl. *Risk*) je svaka prijetnja na koju je mrežni i informacijski sustav ranjiv. Rizik je kombinacija vjerojatnosti nekog događaja i njegovih posljedica odnosno utjecaja. Rizik se najbolje opisuje skupinom pitanja:

1. Što se može dogoditi? (Što je prijetnja?)

2. Koliko teško može biti? (Koliki je utjecaj ili posljedica?)

3. Koliko često se može dogoditi? (Kolika je frekvencija?)

4. Koliko su pouzdani odgovori na prva tri pitanja? (Koliki je stupanj izvjesnosti?)

(17) **Upravljanje rizikom** (engl. *Risk Management*) je pojam koji obuhvaća cjelokupni kontinuirani proces koordiniranih aktivnosti za usmjeravanje i kontrolu organizacije u odnosu na rizik.

(18) **Procjenjivanje rizika** (engl. *Risk Assesment*) je sveukupni proces analize rizika i njihovog vrednovanja. Služi za određivanje vrijednosti imovine, frekvencije prijetnji, procjenu utjecaja na imovinu i drugih faktora vjerojatnosti događanja.

(19) **Identificiranje rizika** (engl. *Risk Identification*) je proces analize i utvrđivanja što i kako se može dogoditi u okruženju od interesa.

(20) **Analiza rizika** (engl. *Risk Analysis*) pruža osnovu za vrednovanje rizika, obradu i prihvaćanje rizika. Povezuje prijetnje, ranjivosti i imovinu, utvrđuje potencijal i prirodu neželjenog događaja, identificira i procjenjuje protumjere za smanjivanje rizika. U određivanju **vjerojatnosti prijetnje** potrebno je razmotriti sve prijetnje, potencijalne ranjivosti i postojeće kontrole mrežnog i informacijskog sustava. Pri tome je važna procjena utjecaja kojim ostvarenje rizika može rezultirati. Analiza **utjecaja** koji je rezultat uspješnog iskorištavanja ranjivosti od strane prijetnje, temelji se na procjeni poslovnih procesa koji se odvijaju na mrežnom i informacijskom sustavu, na kritičnosti određenog sustava i podataka u smislu vrijednosti ili važnosti za subjekt, kao i na osjetljivost sustava i podataka od neovlaštenog pristupa. Općenito se štetni utjecaj nekog incidenta može opisati i u pojmovima gubitka ili degradacije nekog od sigurnosnih kriterija cjelovitosti, raspoloživosti i povjerljivosti. Neki utjecaji se izražavaju kvantitativno, kao npr. gubitak u prihodu ili troškovi oporavka sustava. Drugi utjecaji (npr. gubitak povjerenja javnosti, gubitak vjerodostojnosti, šteta interesima subjekta) se uobičajeno izražavaju kvalitativno pojmovima visokog, srednjeg ili niskog nivoa utjecaja.

(21) **Vrednovanje rizika** (engl. *Risk Evaluation*) je proces usporedbe procijenjenog rizika i danih kriterija rizika kako bi se odredilo značenje rizika u konkretnom okruženju.

(22) **Kriteriji rizika** (engl. *Risk Criteria*) su referentni uvjeti prema kojima se procjenjuje značenje rizika, a mogu uključivati pridružene troškove, zakonske zahtjeve, socioekonomska gledišta i okolinu, druge podatke koji se tiču zainteresiranih strana, prioritete i ostale ulazne podatke potrebne za procjenjivanje.

(23) **Mrežni i informacijski sustav kao imovina podložna rizicima kibernetičke sigurnosti** (engl. *Network and Information System*), sadrži više elemenata direktne ili indirektne vrijednosti imovine koje treba razmotriti: vrijednost zamjenskog elementa ili popravka, trošak zamjene i povrata podataka na informacijskom sustavu, trošak zamjene programske podrške, skup troškova povezanih

s gubitkom povjerljivosti, raspoloživosti i cjelovitosti podataka. Na taj način računa se **vrijednost imovine** (engl. *Asset Value*).

(24) **Prijetnja** (engl. *Threat*) je potencijalni uzrok slučaja koji može naškoditi sustavu ili organizaciji i koji može uzrokovati jednu ili više pojava kao što su neautorizirano otkrivanje, uništenje, uklanjanje, promjenu ili prekid osjetljivih informacija, opreme ili usluga, ili ozljedu ljudi, pri čemu prijetnja može biti namjerna ili slučajna. Prijetnja ne predstavlja rizik kada nema ranjivosti koja se može iskoristiti.

Prijetnje mogu biti:

a) prirodne prijetnje – poplave, potresi, tornada, odroni zemlje, lavine, električne oluje i drugi slični događaji;

b) ljudske prijetnje – događaji koji su ili omogućeni ili uzrokovani od strane ljudskih bića, kao što su nenamjerna djelovanja (npr. nepažljiv unos podataka) ili namjerne aktivnosti (npr. kibernetički napad);

c) prijetnje iz okoline – dugotrajni nestanci napajanja, zagađenje, kemikalije, istjecanje tekućina i sl.

(25) **Ranjivost** (engl. *Vulnerability*) je greška ili slabost u sigurnosnim procedurama, dizajnu, primjeni ili internim kontrolama sustava koja se može nenamjerno ili namjerno iskoristiti za kompromitaciju mrežnog i informacijskog sustava.

(26) **Sigurnosna mjera ili sigurnosna kontrola** (engl. *Security Measure, Countermeasure, Security Control*) predstavlja mjeru smanjenja rizika otkrivanjem, prevencijom, odvraćanjem ili korekcijom. ZKS postavlja zahtjeve za sigurnosne mjere koje su razrađene u Prilogu II. Uredbe i to kao skupina od 13 mjera, koje su podijeljene na podmjere, a mogu se i dalje podijeliti na sigurnosne kontrole, kako je to napravljeno u okviru Smjernica za provedbu samoprocjene kibernetičke sigurnosti, koje je objavio Zavod za sigurnost informacijskih sustava na svojim mrežnim stranicama (https://www.zsis.hr).

(27) **Jednokratni očekivani gubitak** (engl. *Single Loss Expectancy* - SLE) određuje novčani gubitak za svaku pojavu prijetećeg događaja. Računa se kao umnožak vrijednosti imovine (engl. *Asset Value* - AV) i faktora izloženosti (engl. *Exposure Factor* - EF): SLE = AV * EF.

(28) **Faktor izloženosti** (engl. *Exposure Factor* - EF) predstavlja veličinu gubitka ili utjecaja na vrijednost imovine. Izražen je u formi očekivanog postotka gubitka vrijednosti imovine pri djelovanju prijetnje.

(29) **Godišnja učestalost pojave prijetnji** (engl. *Annualized Rate of Occurence* - ARO) predstavlja frekvenciju kojom se očekuje pojava prijetnji na godišnjoj razini.

(30) **Godišnji očekivani gubitak** (engl. *Annualized Loss Expectancy* - ALE) određuje godišnji novčani gubitak za procjenu pojave prijetećeg događaja. Računa se kao umnožak: ALE = SLE * ARO.

(31) **Obrada rizika** (engl. *Risk Treatment*) je proces obrade, odabira i primjene mjera za promjenu rizika. Koriste se odluke o izbjegavanju rizika (engl. *Risk Avoidance*), o modificiranju rizika (engl. *Risk Reduction/Modification*), prihvaćanju rizika (engl. *Risk Retention/Acceptance*) ili dijeljenju rizika (engl. *Risk Sharing*).

(32) **Izbjegavanje rizika** (engl. *Risk Avoidance*) je odluka da se ne ulazi u rizičnu situaciju ili aktivnosti koje su rizične.

(33) **Modificiranje rizika** (engl. *Risk Modification*) predstavlja poduzete akcije u cilju promjene vjerojatnosti pojave nekog događaja, ili promjene razine negativnih posljedica rizika (utjecaj na imovinu).

(34) **Prihvaćanje rizika** (engl. *Risk Retention*/*Acceptance*) je informirana odluka o prihvaćanju procijenjenog i analiziranog rizika.

(35) **Dijeljenje rizika** (engl. *Risk Sharing*) je dijeljenje tereta gubitaka nastalih u svezi s rizikom s drugom stranom koja može biti eksternalizirani davatelj usluga ili osiguravatelj. Potrebno je napomenuti kako odgovornost za rizike kibernetičke sigurnosti uvijek ostaje na subjektu, odnosno odgovornoj osobi subjekta prema točki (13) ovih Smjernica, a dijeljenje se odnosi isključivo na mogućnost ugovorne eksternalizacije nekih aktivnosti u cilju postizanja kibernetičke sigurnosti, ili ugovorno pokrivanje štete nastale kibernetičkim incidentom.

(36) **Preostali rizik** (engl. *Residual Risk*) je rizik koji preostaje nakon primjene novih ili proširenih kontrola. Ako preostali rizik nije bio smanjen na prihvatljivi nivo koji je subjekt odredio kao razinu koja se može tolerirati (engl. *Risk Apetite*), ciklus upravljanja rizikom se mora ponoviti da bi se identificirao način daljnjeg smanjenja preostalog rizika na prihvatljivi nivo.

VI. Pristupi, metode i tehnike koje se koriste u procjeni rizika

(37) Najčešće korištene norme u području upravljanja rizikom su smjernice ISO 31000 i ISO 27005. ISO 31000 predstavlja općenite smjernice za upravljanje rizikom na poslovnoj razini bilo koje organizacije. ISO 27005 predstavlja smjernice za upravljanje rizikom vezanim za informacijsku sigurnost i prvenstveno u okviru provedbe norme ISO 27001. S obzirom na usku povezanost standarda i najboljih praksi koje se koriste u području informacijske i kibernetičke sigurnosti, ove smjernice su u potpunosti iskoristive za upravljanje kibernetičkim sigurnosnim rizicima, odnosno za integrirani pristup upravljanja poslovnim i kibernetičkim rizicima.

(38) Neovisno o korištenoj smjernici za procjenu rizika, potrebno je koristiti utvrđenu razinu mjera kibernetičke sigurnosti za subjekt ZKS-a iz kojeg proizlaze mjere, podmjere, odnosno kontrole koje treba koristiti (označene slovom A u tablicama u Prilogu II. Uredbe), a pored ovih obaveznih mjera mogu se koristiti i druge podmjere iz Uredbe (označene slovom C u tablicama u Prilogu II. Uredbe), kao i kontrole iz nekih drugih normi i najboljih praksi (Smjernica s korelacijskim pregledom mjera koje je objavio NCSC-HR na svojim mrežnim stranicama, https://www.ncsc.hr).

(39) Postoje dva temeljna pristupa procjenjivanju rizika, kvalitativni i kvantitativni. Danas se u praksi puno češće primjenjuje kvalitativni pristup, jer je za većinu primjena jednostavniji, dok se kvantitativni pristup uglavnom koristi u slučajevima primjene nekih složenijih alata za upravljanje rizikom. Skale vjerojatnosti se najčešće koriste na tri ili pet razina za kvalitativne razine vjerojatnosti i utjecaja (npr. mali, srednji, veliki).

(40) Procjena rizika se mora organizirati na formalizirani način u smislu planiranja, načina provedbe i dokumentiranja te periodičkog ponavljanja procesa. Rizik ima vjerojatnost i utjecaj. Vjerojatnost se odnosi na prijetnju koja iskorištava ranjivost, a utjecaj na svu imovinu koja može biti iskorištena ostvarenjem rizika. Uobičajene skale za procjenu vjerojatnosti su: nisko, srednje, visoko, kao i za procjenu utjecaja, što daje pet razina rizika prema Slici 6., koje uobičajeno definiraju razine prioriteta za obradu rizika, odnosno možebitnu prihvatljivost niskih razina za prihvaćanje rizika.

VJEROJATNOST	Visoko	Srednji rizik	Visoki rizik	Vrlo visoki rizik
	Srednje	Niski rizik	Srednji rizik	Visoki rizik
	Nisko	Vrlo niski rizik	Niski rizik	Srednji rizik
		Nisko	Srednje	Visoko
	UTJECAJ			

Slika 6. - Matrica rizika

(41) Za potrebe analize imovine u smislu potencijalne ranjivosti, važnosti i vrijednosti, koriste se tehnike prikupljanja podataka korištenjem prikladnih upitnika, razgovori s odgovornim osobljem (vlasnici poslovnih procesa), kao i uporaba programskih alata. Preporučene metode za identificiranje ranjivosti sustava su upotreba otvorenih izvora informacija o ranjivostima te sigurnosno testiranje sustava. Proaktivne metode koje koriste testiranje sustava mogu se upotrijebiti za učinkovito identificiranje ranjivosti sustava, ovisno o kritičnosti IT sustava i raspoloživih resursa. Metode

testiranja mogu koristiti automatizirane alate za skeniranje ranjivosti, sigurnosno testiranje i procjenu, kao i penetracijsko testiranje. Imovinu je potrebno grupirati u kategorije prema zahtjevima iz točke 2. Priloga II. Uredbe.

(42) Prijetnje je potrebno identificirati u odnosu na utvrđenu imovinu prema točki 41. ovih Smjernica. Pri tome je potrebno koristiti sve vrste prijetnji (engl. *All Hazards Approach*), odnosno pristup koji se temelji na otkazima ili kvarovima (engl. *Failures*) opreme, na mogućim nesrećama (engl. *Accidents*), ili napadima (engl. *Attacks*). U području kibernetičkih sigurnosnih rizika, motivacija i široka raspoloživost alata koji se mogu koristiti za izvođenje kibernetičkih napada, kao i visoka složenost tehnologije, čini ljude posebno opasnim izvorima prijetnje.

(43) Utjecaj ostvarenih rizika na imovinu (mrežni i informacijski sustavi) u prvom redu odnosi se na gubitak ili degradaciju ključnih svojstava povjerljivosti, cjelovitosti i raspoloživosti podataka i usluga. Pri analizi je dodatno potrebno uzeti u obzir i poslovne, pravne i ugovorne utjecaje, kao i moguću reputacijsku štetu.

(44) Vjerojatnost pojave prijetnje, prikazana na Slici 6., uobičajeno se u većini različitih smjernica i najboljih praksi upravljanja rizikom procjenjuje na temelju povijesnih, odnosno raspoloživih statističkih podataka (primjerice prijetnja od potresa ili od neke vrste kibernetičkog napada na nekom području i u nekoj djelatnosti).

(45) Obrada rizika je proces obrade, odabira i primjene kibernetičkih sigurnosnih mjera u cilju željene promjene rizika. Koriste se odluke o izbjegavanju rizika, o smanjenju rizika, prihvaćanju rizika ili dijeljenju rizika te se u tu svrhu provode mjere, podmjere i kontrole kibernetičke sigurnosti te sklapaju ugovorni odnosi. Prema Slici 3. mjere kibernetičke sigurnosti imaju funkciju prevencije, korekcije, detekcije i odvraćanja prijetnji. Pri tome neke mjere predstavljaju obavezu primjene, kao što je to u slučaju ZKS-a obvezujuća razina mjera utvrđena kategorizacijom subjekta (osnovna, srednja ili napredna).

(46) U okviru upravljanja rizikom moguće je koristiti pristup procjeni rizika temeljen na prepoznavanju operativnih rizika za imovinu iz inventara subjekta (engl. *Asset-based Approach*). Imovina koja se razmatra u ovom slučaju su komponente mrežnih i informacijskih sustava. Drugi pristup je temeljen na scenarijima i prepoznavanju izvora strateških rizika za poslovanje subjekta (engl. *Event-based Approach*) te se ovakav pristup temelji na poslovnoj imovini, odnosno poslovnim podacima i procesima od vrijednosti za subjekt. Ovaj drugi pristup može imati prednosti u slučaju subjekta koji ima dosta iskustva u upravljanju rizikom u svom poslovnom okruženju, a za subjekte koji uspostavljaju prvi puta proces upravljanja rizicima preporuča se prvi pristup preko imovine iz inventara subjekta.

(47) Za potrebe upravljanja kibernetičkim sigurnosnim rizikom mogu se koristiti elementi iz Smjernice za nadležna tijela o nacionalnoj procjeni kibernetičkih sigurnosnih rizika koje je objavio NCSC-HR na svojim mrežnim stranicama (https://www.ncsc.hr), kao što su: kategorije kibernetičkih napada, vrste kibernetičkih napadača, kao i kvantificirane vrijednosti određene za sektor u kojem subjekt obavlja svoju djelatnost.

VII. PRILOG – Primjeri tipičnih prijetnji i ranjivosti

(48) U prilogu su dani primjeri tipičnih prijetnji i ranjivosti koji se mogu koristiti kao najmanji preporučeni skup ili prema potrebi proširiti za korištenje subjekta ZKS-a u okviru upravljanja rizikom kroz pristup temeljen na prepoznavanju rizika za imovinu iz inventara subjekta.

Tablica 1. – Primjeri tipičnih prijetnji:

R.br.	Kategorija	Prijetnja
1.	Fizičke prijetnje	Vatra
2.		Voda
3.		Onečišćenje i radijacija
4.		Velika nesreća
5.		Eksplozija
6.		Prašina, korozija, smrzavanje
7.	Prirodne prijetnje	Vremenske nepogode
8.		Potres
9.		Poplava
10.		Pandemije/epidemije
11.	Kvarovi infrastrukture	Kvar u sustavu opskrbe
12.		Kvar sustava za hlađenje ili ventilaciju
13.		Nestanak električne energije
14.		Kvar javne elektroničke komunikacijske mreže
15.		Kvar komunikacijske opreme
16.		Kvar uređaja ili sustava
17.	Ljudske aktivnosti	Teroristički napad, sabotaža
18.		Socijalni inženjering
19.		Prisluškivanje
20.		Krađa podatkovnih medija ili dokumenata
21.		Krađa opreme

22.		Krađa digitalnih identiteta ili vjerodajnica
23.		Iskorištavanje recikliranih ili odbačenih medija
24.		Objava informacija
25.		Unos podataka iz nepouzdanih izvora
26.		Nedozvoljena manipulacija uređajima ili programima
27.		Kibernetički napadi na mrežni i informacijski sustav
28.		Neovlaštena obrada osobnih podataka
29.		Neovlašten ulazak u objekte i prostore
30.		Neovlašteno korištenje uređaja
31.		Neispravno korištenje uređaja
32.		Oštećivanje uređaja ili podatkovnih medija
33.		Neovlašteno kopiranje programskog koda
34.		Korištenje neovlašteno kopiranih podatkovnih medija i programskog koda
35.		Namjerna promjena podataka
36.		Ilegalna obrada podataka
37.		Slanje ili distribuiranje malicioznih programa
38.	Kompromitacija funkcija ili usluga	Pogreška pri korištenju
39.		Zlouporaba prava i dopuštenja
40.		Krivotvorenje prava i dopuštenja
41.		Onemogućavanje aktivnosti
42.	Organizacijske prijetnje	Manjak osoblja
43.		Manjak resursa
44.		Problemi s davateljima usluga
45.		Kršenje zakona i propisa

Tablica 2. – Primjeri tipičnih ranjivosti:

R.br.	Kategorija	Ranjivost
1.	Sklopovske ranjivosti	Nedovoljno održavanje/neispravna instalacija medija za pohranu
2.		Nedovoljne sheme za periodičnu zamjenu opreme
3.		Osjetljivost na vlagu, prašinu, prljavštinu
4.		Osjetljivost na elektromagnetsko zračenje
5.		Nedovoljna kontrola promjena konfiguracije
6.		Osjetljivost na naponske promjene
7.		Osjetljivost na temperaturne promjene
8.		Nezaštićena pohrana
9.		Nekontrolirano bacanje dotrajalih uređaja
10.	Programske ranjivosti	Nedostatno ili nepostojeće testiranje programske podrške
11.		Dobro poznati nedostaci u softveru
12.		Neodjavljivanje prilikom napuštanja radne stanice
13.		Bacanje ili ponovno korištenje podatkovnih medija bez prikladne procedure brisanja
14.		Nedovoljna konfiguracija dnevničkih zapisa potrebnih za praćenje ispravnosti rada mrežnog i informacijskog sustava
15.		Pogrešna dodjela prava pristupa
16.		Korištenje aplikativnih programskih rješenja s visokim privilegijama za pristup podacima u nepredviđenim vremenskim okvirima
17.		Složeno korisničko sučelje
18.		Nedostatna dokumentacija
19.		Neispravne postavke parametara
20.		Neispravni datumi
21.		Nedostatni mehanizmi identifikacije i autentifikacije
22.		Nezaštićene tablice lozinki
23.		Loše upravljanje lozinkama
24.		Omogućavanje nepotrebnih programskih usluga

25.		Nezrelost novih programskih rješenja
26.		Nejasne ili nepotpune specifikacije za razvojne timove
27.		Neučinkovita kontrola promjena mrežnog i informacijskog sustava
28.		Nekontrolirano omogućavanje preuzimanja i korištenja programskih rješenja
29.		Nedostajuće ili nekompletne kopije za povratak programskih i podatkovnih elemenata mrežnog i informacijskog sustava
30.	Mrežne ranjivosti	Nedostatni mehanizmi za potvrdu slanja i primanja poruka
31.		Nezaštićene komunikacijske veze
32.		Nezaštićen osjetljivi mrežni promet
33.		Loše kabliranje
34.		Jedinstvena točka kvara
35.		Neučinkoviti ili nedostajući mehanizmi za identifikaciju i autentifikaciju pošiljatelja i primatelja
36.		Nesigurna mrežna arhitektura
37.		Prijenos otvorenih lozinki
38.		Neadekvatno upravljanje mrežom
39.		Nezaštićene mrežne veze na javne sustave
40.	Ranjivosti osoblja	Nedostatno osoblje
41.		Neadekvatne procedure zapošljavanja
42.		Nedovoljna sigurnosna obuka
43.		Neispravno korištenje programske i sklopovske podrške
44.		Niska razina sigurnosne svijesti
45.		Nedostatni mehanizmi nadzora rada
46.		Nenadzirani rad vanjskog i pomoćnog osoblja
47.		Neučinkovite ili nedostatne politike za ispravnu upotrebu javnih medija i poruka
48.	Ranjivosti objekata i prostora	Neadekvatna ili nepažljiva upotreba fizičke kontrole pristupa zgradama i prostorijama
49.		Lokacije s mogućnošću poplave
50.		Nestabilna električna mreža

51.		Nedostatna fizička zaštita zgrade, prozora i vrata
52.	Ranjivosti u organizaciji subjekta ZKS-a	Formalni postupak za registraciju i odjavu korisnika nije razvijen ili je njegova provedba neučinkovita
53.		Formalni postupak za pregled (nadzor) prava pristupa nije razvijen ili je njegova provedba neučinkovita
54.		Nedovoljne odredbe (u vezi sa sigurnošću) u ugovorima s kupcima i/ili trećim stranama
55.		Postupak praćenja kapaciteta resursa za obradu podataka nije razvijen ili je njegova provedba neučinkovita
56.		Revizije (nadzor) se ne provode redovito
57.		Postupci za identifikaciju i procjenu rizika nisu razvijeni ili je njihova provedba neučinkovita
58.		Nedovoljna ili nikakva izvješća o greškama zabilježena u zapisnicima administratora i operatera pojedinih elemenata mrežnog i informacijskog sustava
59.		Neadekvatne usluge održavanja programske i sklopovske opreme
60.		Nedovoljan ili nepostojeći ugovor o razini usluge
61.		Postupak kontrole promjena nije razvijen ili je njegova provedba neučinkovita
62.		Formalni postupak za kontrolu politika kibernetičke sigurnosti nije razvijen ili je njegova provedba neučinkovita
63.		Formalni postupak za nadzor zapisa politika kibernetičke sigurnosti nije razvijen ili je njegova provedba neučinkovita
64.		Formalni postupak za autorizaciju javno dostupnih informacija nije razvijen ili je njegova provedba neučinkovita
65.		Nepravilna raspodjela odgovornosti u okviru kibernetičke sigurnosti
66.		Planovi kontinuiteta poslovanja ne postoje, ili su nepotpuni, ili su zastarjeli
67.		Pravila korištenja e-pošte nisu razvijena ili je njihova provedba neučinkovita
68.		Postupci za uvođenje nove programske podrške u sustave koji su u korištenju nisu razvijeni ili je njihova implementacija neučinkovita
69.		Postupci za korištenje posebnih skupova osjetljivih vrsta podataka nisu razvijeni ili je njihova provedba neučinkovita
70.		Odgovornosti za kibernetičku sigurnost nisu prisutne u opisima poslova i ugovorima sa zaposlenicima
71.		Disciplinski postupak u slučaju kibernetičkih incidenata nije definiran ili ne funkcionira ispravno
72.		Formalna politika o korištenju mobilnih računala nije razvijena ili je njezina provedba neučinkovita
73.		Nedovoljna kontrola imovine subjekta ZKS-a izvan njegovih poslovnih prostora

74.		Nedovoljna ili nepostojeća politika „čistog stola i čistog ekrana“
75.		Autorizacija za obradu podataka nije implementirana ili ne funkcionira ispravno
76.		Mehanizmi praćenja sigurnosnih propusta nisu pravilno implementirani
77.		Postupci za prijavljivanje sigurnosnih slabosti nisu razvijeni ili je njihova provedba neučinkovita
78.		Postupci za usklađenost odredbi s intelektualnim pravima nisu razvijeni ili je njihova provedba neučinkovita

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