EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ANALIZA IN UPRAVLJANJE TVEGANJ

Božidar DAJČMAN, ICS-Ljubljana

28 | 01 | 2026

ANALIZA TVEGANJ

Postopek upravljanja tveganj na področju informacijske varnosti omogoča prepoznavanje in **vrednotenje pomembnosti tveganj**, ki ogrožajo poslovanje organizacije.

Na podlagi rezultatov analize tveganj se določijo primerne strategije obravnave, prioritete ter ukrepi. Analiza tveganj je torej **podlaga za odločanje**.

IZBIRA METODOLOGIJE

Med **obvezno dokumentacijo**, ki jo predpisuje ZinfV-1 je »Analiza obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisom uporabljene metodologije« (21. člen).

Metodologija analize ni predpisana, vendar tako kot za vse ukrepe velja načelo, da zavezanci za zagotovitev skladnega izvajanja ukrepov največji možni meri in skladno z **najboljšimi razpoložljivimi praksami** ter tudi priporočili in smernicami agencije ENISA uporabljajo evropske in **mednarodne standarde** in tehnične specifikacije (28. člen).

Predstavljena je metodologija iz vzorčnega dokumenta **»Metodologija upravljanja tveganja na področju informacijske varnosti«**, ki temelji na zahtevah Zakona o informacijski varnosti (ZInfV-1) ter standardih ISO/IEC 27001:2022 in ISO/IEC 27005:2022.

METODOLOGIJA

Upravljanje tveganj se izvaja

- sistematično in strukturirano,
- na ravni (ključnih) informacijskih sredstev (npr. strežniki, končne naprave, aplikacije, omrežje, baze podatkov).
- Za vsako sredstvo se ocenjuje vpliv na zaupnost, celovitost, razpoložljivost in avtentičnost (**ZCRA**), verjetnost uresničitve grožnje ter posledice za poslovanje.
- Rezultat je kvantitativna ocena tveganj po modelu 5×5.

METODOLOGIJA

Analiza tveganj se izvaja **v okviru SUVI** organizacije in je usklajena s Politiko informacijske varnosti.

Vključuje **notranji in zunanji kontekst**: zakonodajo, pogodbene zahteve, organizacijsko strukturo, posebnosti področja, tehnološko okolje ter zunanje deležnike in dobavitelje.

Analiza se izvaja **v okviru procesov**, **na nivoju informacijskih sredstev**. To omogoča podrobno identifikacijo in vrednotenje tveganj, povezanih z vsakim sredstvom ali skupino sredstev ter njegovim lastnikom.

OCENA PO SREDSTVIH

Za vsako sredstvo ali skupino (enakih) sredstev se ugotavljajo:

- **grožnje in ranljivosti**;
- **vpliv** na izgubo zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA);
- **verjetnost** uresničenja grožnje ter posledice za poslovanje in
- **ocena (faktor) tveganja** in ustrezni ukrepi za njegovo zmanjšanje ali sprejem.

KLJUČNE FAZE UPRAVLJANJA TVEGANJ

1) **Identifikacija** oziroma ugotavljanje tveganj (prepoznavanje informacijskih sredstev, groženj, ranljivosti in možnih posledic njihovega uresničenja);
2) **Merjenje** oziroma **ocenjevanje tveganj** (določita se verjetnost uresničitve posamezne grožnje in posledično tveganja ter vpliv na poslovanje);
3) **Obvladovanje tveganj** (za vsako tveganje se določi ustrezna strategija: zmanjšanje, prenos, sprejem ali izogib; izvedejo se ukrepi in določijo se odgovorne osebe ter roki);
4) **Spremljanje** tveganj (redno se preverjajo uspešnost izvedenih ukrepov, stanje tveganj in spremembe v poslovnem, tehničnem ali zakonodajnem okolju);
5) **Poročanje** vodstvu o tveganjih (o stanju tveganj in uspešnosti ukrepov se redno poroča vodstvu in odgovorni osebi za informacijsko varnost).

METODOLOGIJA ZA IZVEDBO OCENE TVEGANJ

Postopek ocene tveganj temelji na poenostavljenem modelu kvantitativne ocene tveganj, ki upošteva ocenjevanje konteksta organizacije, vrednosti sredstev, ocenjuje **verjetnost realizacije grožnje** in s tem pojava tveganja in **vpliv na poslovanje**.

Metodologija temelji na modelu 5×5, kjer je bistveni faktor vpliva pomembnost sredstva (ocena 1 do 5). Tak pristop vključuje
- opredelitev meril sprejemljivosti tveganj,
- razlikovanje med inherentnim in rezidualnim tveganjem ter
- določitev vlog in odgovornosti.

Vsako tveganje ima določene: lastnika sredstva, lastnika tveganja, izvajalca ukrepov in osebo, ki odobri **sprejemljivo raven tveganja**.

Za vsako tveganje se najprej oceni **inherentno** tveganje (brez kontrol), nato se pri oceni upoštevajo že uvedene kontrole ter se tako oceni oziroma določi **rezidualno** (preostalo) tveganje, ki je osnova za odločitev o sprejemu, zmanjšanju ali prenosu tveganja.

KORAKI POSTOPKA OCENE TVEGANJ (1/2)

1. Identifikacija sredstev – določijo se informacijska sredstva, njihove lastnosti in lastniki.

2. Ocena vpliva na sredstvo - določi se vpliv na poslovanje oziroma pričakovane posledice v primeru uresničitve grožnje na sredstvo, zapiše se ocena ZCRA, ki je določena v seznamu informacijskih virov (vpliv na zaupnost, celovitost, razpoložljivost in avtentičnost). Ocena ZCRA določa lestvico vpliva - lestvica od 1 do 5.

3. Prepoznava groženj in ranljivosti - za vsako sredstvo se določi grožnja in ranljivost (uporaba relevantnih obveščevalnih podatkov, obvestil CSIRT in URSIV, ocen ali samoocen skladnosti in podatkov dobaviteljev) - lestvica od 1 do 5.

4. Ocena verjetnosti – določi se pogostost oziroma verjetnost uresničitve grožnje (brez uvedenih ukrepov in kontrol) - lestvica od 1 do 5.

5. Izračun inherentnega tveganja – Faktor (inherentnega) tveganja = **Vpliv × Verjetnost** (brez uvedenih ukrepov in kontrol) - lestvica od 1 do 25.

KORAKI POSTOPKA OCENE TVEGANJ (2/2)

6. Določitev sprejemljive stopnje tveganj – vodstvo organizacije določi sprejemljivo stopnjo tveganj.

7. Navedba ukrepov in kontrol, ki so že uvedene.

8. Ocena verjetnosti uresničitve grožnje po izvedenih ukrepih oziroma kontrolah.

9. Izračun preostalega tveganja – Faktor (rezidualnega) tveganja = **Vpliv × Verjetnost** (po izvedenih ukrepih oziroma kontrolah) - lestvica od 1 do 25.

10. Določitev ukrepov in kontrol, ki jih je treba izvesti za znižanje faktorja (preostalega)

tveganja (obvezno, če je faktor tveganja nad sprejemljivo ravnijo tveganja).

11. Določitev prioritet ukrepov – na podlagi faktorja preostalega (rezidualnega) tveganja se določi strategija obravnave posameznega tveganja.

LESTVICA OCEN VPLIVA

3.2 Lestvica vpliva (1–5)

Ocena	Opis	Primer posledic
1	Zanemarljiv	Vpliv na sredstvo ne povzroči poslovne motnje (najvišja ocena ZCRA je 1). Brez opaznega vpliva na poslovanje.
2	Majhen	Vpliv na sredstvo vpliva le na posameznika ali del organizacijske enote (najvišja ocena ZCRA je 2). Manjše motnje ali zelo omejen vpliv.
3	Srednji	Vpliv na sredstvo privede do motenj delovanja, a poslovanje ostane vzdržno (najvišja ocena ZCRA je 3). Kratkotrajne motnje, manjši vpliv na posamezno organizacijsko enoto.
4	Visok	Vpliv na sredstvo vpliva na ključne procese, verjetne so zakonske neskladnosti ali negativen vpliv na ugled (najvišja ocena ZCRA je 4). Motnje ključnih procesov, finančni vpliv, izguba podatkov v manjšem obsegu.
5	Kritičen	Vpliv na sredstvo ima resne posledice, poslovanje je onemogočeno, pravne in finančne posledice (najvišja ocena ZCRA je 5). Prekinitev poslovanja, velik finančni vpliv, izguba podatkov, izguba ugleda.

LESTVICA OCEN VERJETNOSTI

3.3 Lestvica verjetnosti (1-5)

Ocena	Opis	Primer
1	Zelo nizka	Dogodek je malo verjeten (1× v 10 letih).
2	Nizka	Redko, vendar možno (1× v 5 letih).
3	Srednja	Občasno (1× na 2 do 3 leta).
4	Visoka	Pogosto (vsaj 1× na leto).
5	Zelo visoka	Pričakovano večkrat letno.

LESTVICA RAZVRSTITEV TVEGANJ

3.4 Lestvica razvrstitve tveganj (1-25)

Faktor tveganja	Stopnja	Opis
1 – 5	Nizko	Sprejemljivo, spremlja se le ob spremembah okolja ali sistema.
6 - 10	Zmerno	Potrebno spremljanje in izvajanje osnovnih ukrepov.
11 – 15	Povišano	Zahteva načrt za zmanjšanje tveganja in določitev odgovorne osebe.
16 – 20	Visoko	Nujna izvedba ukrepov v kratkem roku in poročanje vodstvu.
21 – 25	Kritično	Tveganje nesprejemljivo, potrebno je takojšnje ukrepanje.

MERILA SPREJEMLJIVOSTI TVEGANJ

Sprejemljivost tveganj je določena z matriko od 1 do 25. Določene meje so: nizko (ukrepi niso potrebni),

- zmerno (potrebno spremljanje in izvajanje osnovnih ukrepov),
- povišano (zahteva se izdelava načrta za zmanjšanje tveganja in določitev odgovorne osebe),
- visoko (nujna uvedba ukrepov in poročanje vodstvu) in
- kritično (potrebni so takojšnji ukrepi).

Pragove sprejemljivosti potrjuje vodstvo ob letnem pregledu. Vodstvo lahko izrecno določi izjeme - katera visoka ali kritična tveganja bo sprejelo kot sprejemljiva. Izjeme (sprejem visokega/kritičnega tveganja) se dokumentirajo z utemeljitvijo, časovno omejitvijo in datumom naslednjega pregleda.

REZULTAT IZVEDENE ANALIZE TVEGANJ IN IZVAJANJE UKREPOV

Rezultat analize tveganj je **register tveganj**.

Vključuje:

- naziv sredstva (ali skupine sredstev) na katerega se tveganje nanaša,
- lastnika sredstva/tveganja,
- opis tveganja,
- vpliv v primeru kršitve zaupnosti, celovitosti, razpoložljivosti in avtentičnosti (ZCRA).
- oceno verjetnosti realizacije grožnje,
- faktor inherentnega tveganja,
- predlagane ukrepe za zmanjšanje tveganj, prenos ali sprejem tveganj,
- faktor rezidualnega tveganja,
- rok za realizacijo ukrepov.

SPREMLJANJE, POSODABLJANJE IN POROČANJE

Analiza tveganj se izvaja **najmanj enkrat letno** ali ob večjih spremembah informacijskega sistema ali prepoznanih incidentih ali spremembah ključnih procesov. Rezultati se beležijo v **register tveganj**.

Za spremljanje uspešnosti izvajanja ukrepov se uporabljajo merljivi kazalniki, kot so: delež izvedenih ukrepov v roku, število odprtih visokih tveganj, delež zmanjšanih tveganj in število ponavljajočih se incidentov.

PREDSTAVITEV PRIMERA OCENJEVANJA TVEGANJ

/primer ocenjevanja – register tveganj (excel)

KAKO ZASTAVITI OBVLADOVANJE TVEGANJ V VAŠI ORGANIZACIJI?

Če je v organizaciji že vpeljan okvir upravljanje tveganj, potem je najbolje, da se upravljanje ostane, oz. se razvije v tem skupnem okviru.

Če začenjate iz nič, je vzorčna metodologija dobra osnova za vašo lastno.

Od stopnje zrelosti organizacije je odvisno, kako podrobno bodo obravnavana informacijska sredstva pri analizi. Če metodologijo šele vzpostavljamo, moramo ostati na dovolj splošnem nivoju, da bomo lahko izpeljali ves cikel in dosegli skladnost.

Organizacije na višjem nivoju zrelosti ocene tveganj izvajajo v neposredni povezavi z registri sredstev ali bazami CMDB. To je zahtevno, ker je zaradi velikega obsega (več tisoč sredstev) potrebna vsaj delna avtomatizacija. Za ta namen je treba definirati in vzdrževati veliko število povezav (npr. med procesi in aplikacijami) in pravila dedovanja.

NEKAJ VPRAŠANJ ZA VSAKO ORGANIZACIJO

Kako določiti lastnike sredstev in tveganj? Kako zagotoviti njihovo aktivno vključenost?

Kako zagotoviti, da bo ocena tveganj realna, neodvisna, in posledično primerna podlaga za odločanje?

Kakšna je povezava med analizo tveganj in procesom upravljanja ranljivosti (vzorčni načrt varnostnih ukrepov, točka 2.13)?

Kako razumeti sorazmernost ukrepov s tveganji, velikostjo organizacije (ZInfV-1, čl. 22.3, 22.13.4) in hkratno uporabo najboljših razpoložljivih praks (ZInfV-1, čl. 28.1)?

Ali je organizacija dodelila dovolj virov za vzpostavitev ustrezne skladnosti in odpornosti?

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HVALA ZA POZORNOST

Agamemnonos 14, Chalandri 15231
Attiki, Greece

osu-ms-support@enisa.europa.eu

www.enisa.europa.eu