

Vzorec dokumenta Ocena varnostnih tveganj

Ocena varnostnih tveganj sistema

- Ime organa:
- Št. dokumenta:
- Datum:
- Naslov dokumenta: Ocena varnostnih tveganj sistema << *ime sistema* >>
- Različica dokumenta:
- Avtorji dokumenta:
- Nadzor (zgodovina) dokumenta:
- Viri:
- Slovar pojmov:
- Kratak povzetek/namen dokumenta:

1. poglavje: Uvod

- ime sistema (kratko, dolgo),
- kratak opis sistema,
- najvišja stopnja tajnih podatkov v sistemu,
- razlaga stopenj ocene tveganja, npr.:

Posamezna varnostna tveganja so v tej oceni razvrščena po verjetnosti dogodka in njegovem vplivu na operativnost sistema "primer" v naslednje stopnje:

	Lestvica verjetnosti negativnega dogodka				
Lestvica kritičnosti	zelo visoka	visoka	zmerna	nizka	zelo nizka
zelo visoka	zelo visoko	zelo visoko	visoko	zmerno	nizko
visoka	zelo visoko	visoko	visoko	zmerno	nizko
zmerna	visoko	visoko	zmerno	nizko	nizko
nizka	zmerno	zmerno	nizko	nizko	zelo nizko
zelo nizka	nizko	nizko	nizko	zelo nizko	zelo nizko

Lestvica kritičnosti:

- zelo visoka, kar pomeni, da organizacija ne more izpolnjevati osnovnega namena delovanja brez uporabe komunikacijsko informacijskega sistema ali podatkov, ki jih obravnava;
- visoka, kar pomeni, da organizacija ne more učinkovito izpolnjevati dela osnovnega namena delovanja brez uporabe komunikacijsko informacijskega sistema ali podatkov, ki jih obravnava;
- zmerna, kar pomeni, da je delovanje organizacije resno ogroženo, vendar lahko osnovni namen delovanja izpolni drugače z zmernimi stroški;
- nizka, kar pomeni, da bi bil ob izgubi ali razpadu komunikacijsko informacijskega sistema ali podatkov, ki jih obravnava, učinek na izpolnjevanje osnovnega namena organizacije majhen;
- zelo nizka, kar pomeni, da komunikacijsko informacijskega sistema ali podatki, ki jih obravnava, niso pomembni za izpolnjevanje osnovnega namena delovanja organizacije.

Lestvica verjetnosti negativnega dogodka:

- zelo visoka, kar pomeni, da se bo dogodek skoraj zagotovo zgodil;
- visoka, kar pomeni, da se bo dogodek verjetno zgodil;
- zmerna, kar pomeni, da se bo dogodek mogoče zgodil;
- nizka, kar pomeni, da se dogodek mogoče ne bo zgodil;
- zelo nizka, kar pomeni, da se dogodek skoraj zagotovo ne bo zgodil.

Priporočljiva sprejemljiva tveganja so: zelo nizka in nizka.

Priporočljiva pogojno sprejemljiva tveganja so: zmerna in visoka.

Nesprejemljiva tveganja so: zelo visoka.

2. poglavje: Ocena trenutnega stanja sistema << ime sistema >> z oceno stopnje tveganja

2.1 Nesreče iz okolja:

- kratek opis tveganja ob nesreči iz okolja, kot so potres, požar, poplava, epidemija, neurja ...,
- ocena stopnje tveganja za nesreče iz okolja,
- opis zagotavljanja celovitosti sistema << ime sistema >> ob nesrečah iz okolja,
- opis zagotavljanja razpoložljivosti in dostopnosti sistema << ime sistema >> ob nesrečah iz okolja,
- opis zagotavljanja zaupnosti sistema << ime sistema >> ob nesrečah iz okolja.

2.2 Organizirano in/ali načrtno poškodovanje:

- kratek opis tveganja ob organiziranem in/ali načrtnem poškodovanju, kot so teroristični napad, sabotaža, vojna, kraja, požig, nezadovoljni zaposleni ...,
- ocena stopnje tveganja za organizirano in/ali načrtno poškodovanje sistema oziroma podatkov v njem,
- opis zagotavljanja celovitosti sistema << ime sistema >> ob organiziranem in/ali načrtnem poškodovanju,
- opis zagotavljanja razpoložljivosti in dostopnosti sistema << ime sistema >> ob organiziranem in/ali načrtnem poškodovanju,
- opis zagotavljanja zaupnosti sistema << ime sistema >> ob organiziranem in/ali načrtnem poškodovanju.

2.3 Izguba storitev javne infrastrukture:

- kratek opis tveganja ob izgubi storitev javne infrastrukture, kot so elektrika in telekomunikacije,
- ocena stopnje tveganja ob izgubi storitev javne infrastrukture,
- opis zagotavljanja celovitosti sistema << ime sistema >> ob izgubi storitev javne infrastrukture,
- opis zagotavljanja razpoložljivosti in dostopnosti sistema << ime sistema >> ob izgubi storitev javne infrastrukture,
- opis zagotavljanja zaupnosti sistema << ime sistema >> ob izgubi storitev javne infrastrukture.

2.4 Strojne in sistemske napake:

- kratek opis tveganja ob strojnih in sistemskih napakah, kot so težave z ožičenjem, klimatizacijo ali odpovedjo vitalnih delov sistema,
- ocena stopnje tveganja ob strojnih in sistemskih napakah,
- opis zagotavljanja celovitosti sistema << *ime sistema* >> ob strojnih in sistemskih napakah,
- opis zagotavljanja razpoložljivosti in dostopnosti sistema << *ime sistema* >> ob strojnih in sistemskih napakah,
- opis zagotavljanja zaupnosti sistema << *ime sistema* >> ob strojnih in sistemskih napakah.

2.5 Varnostno in poslovno nepredvidljivi dogodki:

- kratek opis tveganja ob varnostno in poslovno nepredvidljivih dogodkih, kot so kibernetični napadi ter izguba, poškodovanje ter razkritje podatkov,
- ocena stopnje tveganja ob varnostno in poslovno nepredvidljivih dogodkih,
- opis zagotavljanja celovitosti sistema << *ime sistema* >> ob varnostno in poslovno nepredvidljivih dogodkih,
- opis zagotavljanja razpoložljivosti in dostopnosti sistema << *ime sistema* >> ob varnostno in poslovno nepredvidljivih dogodkih,
- opis zagotavljanja zaupnosti sistema << *ime sistema* >> ob varnostno in poslovno nepredvidljivih dogodkih.