

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

ZAKON O INFORMACIJSKI VARNOSTI

KAJ PRIČAKOVATI OB OBISKU INŠPEKTORJA

Vojka Jesenko, inšpektorica višja svetnica, Inšpekcija za informacijsko varnost

Portorož, maj 2026

URSIV

CILJI

- RAZUMEVANJE OBVLADOVANJA PROCESOV IN INFORMACIJSKIH SREDSTEV – ANALIZA VPLIVA NA POSLOVANJE IN OCENA TVEGANJ
- KAKO ZAKON LAHKO POMAGA PRI POSLOVANJU Z DOBAVITELJI – VARNOST DOBAVNE VERIGE
- ZAKAJ ODGOVORNOSTI NI DOBRO PRENAŠATI NA DRUGE

URSIV

ZAKAJ SO KABELSKI OPERATERJI ZAVEZANCI ?

- ponudniki javnih elektronskih komunikacijskih omrežij in storitev
- omrežna infrastruktura, distribucija komunikacijskih storitev, kritičnost komunikacijskih povezav, ip telefonija

- motnje storitev kabelskih operaterjev lahko vplivajo na javno varnost, kar pomeni lahko širše gospodarske in družbene posledice

- **RAZPOLOŽLJIVOST STORITVE JE TVEGANJE, KI LAHKO OGROZI OBSTOJ KABELSKEGA OPERATERJA**

URSIV

ZAKAJ SO KABELSKI OPERATERJI ZAVEZANCI ?

- **povezava do samoregistracije :**

URSIV

ZAKONSKE OBVEZE

- ODGOVORNOSTI VODSTVA – 20. ČLEN
- VARNOSTNA DOKUMENTACIJA – 21. ČLEN

VZORČNA DOKUMENTACIJA JE DOSTOPNA NA

https://www.gov.si/novice/2025-12-12-vzorcna-varnostna-dokumentacija-za-organizacije/

- VARNOSTNI UKREPI – 22. ČLEN
- OCENA SKLADNOSTI – 25. ČLEN
- UKREPANJE OB INCIDENTIH – 30. ČLEN

URSIV

VLOGA VODSTVA

- ZAGOTAVLJA SKLADNOST SUVI/SUNP S STRATEGIJO ORGANIZACIJE (OBSEG, KRITIČNOST PROCESOV, MINIMALNA RAVEN POSLOVANJA, SPREJEMLJIVI NIVO TVEGANJ PO METODOLOGIJAH, KI JIH ODOBRI VODSTVO)
- ZAGOTAVLJA DVIG VARNOSTNE KULTURE -> USPOSOBLJENOST KADRA
- ODOBRI UKREPE IN NADZIRA NJIHOVO IZVAJANJE
- ZAGOTAVLJA VIRE ZA IZVEDBO



URSIV

VARNOSTNA DOKUMENTACIJA KOT TEMELJNI VARNOSTNI VIDIK

- ZAUPNOST, RAZPOLOŽLJIVOST, CELOVITOST, AVTENTIČNOST – ZRCA / CIAA
  - določitev kritičnosti procesov - izdelava analize vpliva na poslovanje - BIA (obvezna določitev minimalne ravni poslovanja)
  - prepoznava - popis informacijskih sredstev - analiza tveganj z upoštevanjem ZRCA načela za sredstvo
  - dokumentirani varnostni postopki
  - upravljanje tveganj in dobavne verige
  - politika neprekinjenega poslovanja z načrti obnovitve

- SKLADNOST Z ZAKONOM

URSIV

SISTEM UPRAVLJANJA NEPREKINJEGA POSLOVANJA

ni dokument, ampak sistem, ki vsebuje:

- kontekst organizacije
- vloge in odgovornosti
- operativne sklope oz. jedra →osnova je popis procesov
  - analiza vplivov na poslovanje (BIA)
  - politika in načrt neprekinjenega poslovanja (BCP)
  - načrt obnovitve in ponovne vzpostavitve (DRP)
- testiranje
- nadzor

URSIV

ANALIZA VPLIVA NA POSLOVANJE - BIA

POSLOVNA /VODSTVENA ODLOČITEV, KAJ JE ZA ORGANIZACIJO BISTVENO ZA OBSTOJ

KAJ NAM BIA POVE?

- ✓ **kateri proces ali storitev je za organizacijo kritičen → "pokaže" najbolj kritična sredstva_**
- ✓ **kako dolgo si lahko organizacija privošči izpad procesa/storitve**
- ✓ **kakšne so posledice izpada skozi čas za organizacijo**

URSIV

GROŽNJE → TVEGANJA

- NABOR GROŽENJ NIKOLI NE VSEBUJE SAMO „CYBER“ GROŽENJ
- OCENA TVEGANJA ZA POSAMEZNO STORITEV ≠ OCENA TVEGANJA ZA POSAMEZNO SREDSTVO
- TVEGANJA SO POSLOVNA DOMENA

- ogrožajo poslovanje organizacije
- posledice niso omejene zgolj na it/ot okolje,
- zakonska in sistemska obveznost

TVEGANJA UPRAVLJA VODSTVO

(in ne IT služba, Copilot, Claude, Grok ali ChatGPT)

URSIV

ZAKAJ INVENTURA NI POPIS SREDSTEV?

NE MORETE UPRAVLJATI, ČESAR NE POZNATE!

- strojna in programska oprema ter IS - tudi verzije opreme
- podatke, ki jih obdelujete
- komunikacijska in oblačna infrastruktura
- identitete in računi, certifikati
- pogodbe, SLA
- AI rešitve in agenti



URSIV

VARNOSTNI UKREPI – 22. ČLEN

MINIMALNO ZAHTEVAN NABOR 17 UKREPOV, KI TEMELJIJO NA PRISTOPU UPOŠTEVANJA VSEH NEVARNOSTI, MORAJO BITI DOKUMENTIRANI, SORAZMERNI, PREVERLJIVI

- podpora vodstva – vključitev v letni načrt poslovanja
- zagotavljanje usposabljanj in izobraževanj
- upravljanje omrežnih in informacijskih sistemov
- varnost človeških virov, preverjanje identitet in upravljanje pooblastil za dostop
- upravljanje prometa in komunikacij
- varnostni mehanizmi v posamezni aplikativni programski opremi
- upravljanje in preprečevanje izrab tehničnih ranljivosti
- varnost dobavne verige
- in ostalih 8 ☺, ki jih najdete v 22. členu zakona

URSIV

DOBAVNA VERIGA

Dobavna veriga je vse, kar operater uporablja, a ni pod njegovim neposrednim nadzorom:

- **DOBAVITELJI OMREŽNE IN IKT OPREME: proizvajalci in distributerji aktivne in pasivne opreme (CMTS, OLT, stikala, usmerjevalniki, strežniki, scada,...).**
- **PONUDNIKI OBLAČNIH IN PODATKOVNIH STORITEV: zagotavljajo gostovanje aplikacij, podatkov ali storitev**
- **PONUDNIKI UPRAVLJANIH IN VARNOSTNIH STORITEV: monitoring, odzivanje na incidente, izvedba penetracijskih testov, varnostni pregledi,...**
- **ZUNANJI IZVAJALCI IN DRUGI POGODBENI PARTNERJI: izvajalci terenskih del, vzdrževanja infrastrukture, računovodski servis,...**

URSIV

VARNOST DOBAVNE VERIGE

- register ključnih dobaviteljev s kontaktnimi podatki
- klasifikacija po kritičnosti
- vključitev varnostnih zahtev v pogodbe
- vključitev dobaviteljev v testiranje načrtov obnovitve in ponovne vzpostavitve kritičnih procesov

- PRIPOMOČEK - SAMOOCENITVENI VPRAŠALNIK →

URSIV

PRIMERI VARNOSTNIH ZAHTEV

- zahteve glede večfaktorske avtentikacije
- upravljanje privilegiranih dostopov,
- obveznost poročanja incidentov,
- pravico do nadzora/revizije,
- zahteve glede načrtov obnovitve in ponovne vzpostavitve
- zahteve glede redundance in varnostnega kopiranja
- nda - varovanje podatkov
- pogoje glede segmentacije dostopov
- pogoje za oddaljeni dostop
- “flow-down” zahteve za podizvajalce

URSIV

OBISK INŠPEKTORJA

INŠPEKCIJSKI POSTOPEK **NI NAMENJEN KAZNOVANJU**,

AMPAK JE **PRILOŽNOST** ZA OBJEKTIVEN PREGLED STANJA IN

IZBOLJŠANJE LASTNE VARNOSTI.

URSIV

OBISK INŠPEKTORJA

POOBLASTILA :

- neposreden vpogled v podatke, dokumentacijo ter v sisteme
- inšpekcijski pregled na kraju ali nadzor na daljavo (eksperti)
- inšpekcijski varnostni pregled (testiranja varnostnih ukrepov)
- preverjanje pogojev in načina izvajanja varnostnih ukrepov
- pregled območij, objektov in prostorov zavezancev, kjer so ključni sistemi ni podatki
- pregled dokumentacije o izvajanju obveščanja o incidentih
- pregled poročil o izvedbi revizije is in izvedbi varnostnih pregledov
- druga pooblastila po zakonu o inšpekcijskem nadzoru

URSIV

INŠPEKCIJSKI POSTOPEK V PRAKSI

FAZA PRIPRAVE:

- pisna najava izvedbe inšpekcijskega nadzora in posredovanje vprašalnika za preliminarno oceno skladnosti
- pridobitev in analiza relevantnih podatkov o zavezancu od drugih organov in organizacij (od pristojnega nacionalnega organa, VOC, SI-CERT, ipd)
- pridobivanje in analiza podatkov iz „odprtih“ in namenskih orodij
- priprava internega načrta in opomnika za izvedbo nadzora

URSIV

INŠPEKCIJSKI POSTOPEK V PRAKSI

FAZA IZVEDBE:

- zbiranje, pregled in presoja internih dokumentov (tudi pogodb)
- razgovori s pristojnimi predstavniki zavezanca in drugimi zaposlenimi
- pregledi lokacij, kjer se izvajajo (it/ot) procesi v povezavi z izvajanjem dejavnosti
- posredovanje pisnih vprašanj zavezancu
- pridobitev in presoja dokazil o izvajanju predpisanih ukrepov
- izvedba različnh testiranj izvajanja predpisanih ukrepov

URSIV

INŠPEKCIJSKI POSTOPEK V PRAKSI

FAZA ZAKLJUČKA:

- zapis ugotovitev nadzora, ukrepov za odpravo nepravilnosti in priporočil v zapisnik o inšpekcijskem pregledu
- izvedba usklajevalnega sestanka s predstavniki zavezanca s predstavitvijo ugotovitev in dogovor o rokih za izvedbo ukrepov
- izvedba notranjega kolegijskega pregleda zapisnika o inšpekcijskem nadzoru (revizijska tveganja)
- podpis in vročitev zapisnika o inšpekcijskem nadzoru zavezancu
- izdaja ureditvene odločbe zavezancu in prekrškovni postopek

URSIV

POGOSTA ZAZNANA NESKLADJA S PREDPISI

- ni izvedenega ustreznega popisa sredstev (pogosto samo delno, nepopolno ali neažurno)
- ni izvedenih popisov poslovnih procesov (ali so izvedeni samo delno), posledično ni izvedene BIA ali je BIA izvedena neustrezno
- ni določene minimalne ravni poslovanja
- neučinkovito izvajanje dolžnega nadzorstva nad pogodbeniki
- nedosledno izvajanje postopkov upravljanja pravic dostopa pri spremembah ali prekinitvah zaposlitve
- neustrezna segmentacija omrežja (ali je sploh ni)
- se ne izvaja rednega izobraževanja/ozaveščanja zaposlenih
- ni zagotovljenih ustreznih usposabljanj in izpopolnjevanj za ključni it kader (skrbniki is)
- ni preverjanja kakovosti izdelave varnostnih kopij
- ni zagotovljeno ohranjanje dnevniških zapisov o delovanju vseh ključnih informacijskih sistemov in delov omrežja

URSIV

KAJ LAHKO NAREDITE TAKOJ?

- popis procesov z informacijskimi sredstvi,
- določitev minimalne ravni poslovanja
- ustrezen popis informacijskih sredstev z analizo tveganja
- vzpostavitev sistema rednega poročanja glede informacijske varnosti
- NAČRTUJTE IN ZAGOTOVITE VIRE ZA OPREMO, USPOSABLJANJA

ČESA NE SMETE NAREDITI?

- upati, da se bo incident zgodil v mandatu vašega naslednika
- prepustiti informacijsko varnost IT službi ali AI – nista odgovorna

URSIV

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

HVALA ZA POZORNOST

Vojka Jesenko
gp.uiv@gov.si

vojka.jesenko@gov.si



URSIV. Kibernetsko varni.