Predstavitev
Zakona o informacijski varnosti (ZInfV)

Barbara Pernuš Grošelj, univ. dipl. iur., Direktorat za informacijsko družbo, Ministrstvo za javno upravo

Zakon o informacijski varnosti (ZInfV) – splošno

ZInfV:

Objavljen v Uradnem listu RS, št. 30 z dne 26. 4. 2018 (začel veljati 11. 5. 2018).

Namen ZInfV:

- prenos **Direktive 2016/1148/EU** o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji**(t.i. Direktiva NIS).** Rok prenosa: 9.5. 2018 ter
- sistemska ureditev področja informacijske varnosti (I.V.) na strateški in operativni ravni zagotavljanja I.V.

Obdelava podatkov na podlagi ZInfV:

- osebni podatki: skladno s predpisi o varstvu osebnih podatkov (GDPR…)
- podatki + informacije, ki so opredeljeni kot tajni ali poslovna skrivnosti: v skladu s predpisi s področja tajnih podatkov in poslovne skrivnosti (ZTP, ZGD)

ZInfV – izključitev uporabe in področja urejanja

IZKLJUČITEV UPORABE ZInfV (skladno z Direktivo NIS) **ZA**:

- za pravne in fizične osebe, v kolikor zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve (operaterji), za katere veljajo posebne obveznosti o varnosti in celovitosti omrežij iz Zakona o elektronskih komunikacijah - ZEKom-1 (prenos t.i. Okvirne direktive);
- ponudnike storitev zaupanja, za katere že veljajo obveznosti iz (19. člena) neposredno uporabljive Uredbe 910/2014/EU o e-identifikaciji in storitvah zaupanja za e-transakcije na notranjem trgu (t.i. Uredba eIDAS).

Pristojnosti in organizacija na področju I.V. -1

PRISTOJNI NACIONALNI ORGAN (PNO): organ v sestavi ministrstva, pristojnega za informacijsko družbo (že predvidena „Uprava RS za informacijsko varnost“):

- **vodi sezname** (o kontaktnih podatkih zavezancev, incidentih in kibernetskih napadih);
- **obvešča javnost** o incidentih in v zvezi z njimi sprejetimi ukrepi;
- **odloča o sprejemu ukrepov** v primeru težjega ali kritičnega incidenta ali v primeru kibernetskega napada, kot tudi v primeru stanja povečane ogroženosti in **odloča v postopkih nadzora**;
- izpolnjuje **mednarodne obveznosti,** opravlja naloge mednarodne izmenjave podatkov, izvaja **naloge enotne kontaktne točke in sodeluje** s pristojnimi organi s področja informacijske varnosti **v EU**;
- **opravlja koordinacijske, strokovno tehnične, organizacijske in razvojne naloge** na področju informacijske varnosti vključno kibernetske obrambe.

PNO – deluje bolj na strateški ravni sistema informacijske varnosti RS

Pristojnosti in organizacija na področju I.V. -2

S PNO sodelujejo in delujejo na operativni ravni zagotavljanja sistema informacijske varnosti:

- **nacionalni CSIRT** (nacionalna skupina za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij) je odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri ARNES;
- **CSIRT organov državne uprave** (skupina za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij v organih državne uprave – v ODU), bo na ministrstvu, pristojnem za upravljanje informacijsko-komunikacijskih sistemov (sedaj MJU) in pristojen, če ODU nimajo v svoji notranje organizacijski strukturi zagotovljene lastne zmogljivosti vsaj na ravni varnostno operativnega centra (VOC);
- **VOC pri ODU** (npr. v okviru MORS, Policije, SOVA…);

Pristojni organi na področju kibernetske obrambe: PNO, nacionalni CSIRT, CSIRT organov državne uprave, MORS, Policija, SOVA idr. nac. organi (usklajujejo in izvajajo kibernetsko obrambo skladno s svojimi pristojnostmi).

ZAVEZANCI

1. IZVAJALCI BISTVENIH STORITEV (IBS)

Značilna neposredna povezanost s fizično infrastrukturo: stopnja tveganja v praksi visoka. Zato so varnostne zahteve strožje + več možnosti nacionalnega urejanja (Direktiva NIS tu zahteva le minimalno harmonizacijo).

2. PONUDNIKI DIGITALNIH STORITEV (PDS)

Stopnja tveganja nižja: blažja določitev/izvajanje ukrepov. Čezmejna narava PDS - bolj harmoniziran pristop EU (tu maksimalna harmonizacija po Direktivi NIS).

3. ORGANI DRŽAVNE UPRAVE (ODU)

Nacionalno urejanje v ZInfV - Direktiva NIS tega področja ne ureja.

1. IZVAJALCI BISTVENIH STORITEV (IBS)

A. Za namen določitve IBS Vlada z Uredbo:
- **določi seznam bistvenih storitev (iz SKD),**
- **podrobnejšo metodologijo za določitev IBS.**

Nato Vlada na podlagi zakonskih meril (7. člen) določi posameznega izvajalca IBS.

B. Vlada za IBS določi še:
- **upravljalce kritične infrastrukture določene po predpisih s področja KI in**
- **nosilce obrambnega načrtovanja, določene po predpisih s področja OBR. ,**

katerih zagotavljanje storitev je odvisno od omrežij in informacijskih sistemov.

energija

promet

zdravstvo

bančništvo

digitalna infrastruktu

IBS delujejo na 7+2 področjih

oskrba s pitno vodo in njena distribucija

infrastruktura finančnega trga

Poleg 7 področij po Direktivi NIS še 2 nacionalno določeni področji:
- preskrba s hrano in
- varstvo okolja

2. PONUDNIKI DIGITALNIH STORITEV (PDS)

PDS so zavezanci neposredno na podlagi ZInfV (se ne določajo posebej s strani Vlade) - maks. harmonizirano v EU (Direktiva NIS)

IZJEMA: ZAVEZANCI NISO PDS, ki imajo manj kot 50 zaposlenih in letni promet oz. letno bilančno vsoto, ki ne presega 10 mio. EUR (mikro ali mala podjetja skladno z merili EU)

Digitalne storitve (DS) le:

- spletna tržnica
- spletni iskalnik
- storitev računalništva v oblaku

3. ORGANI DRŽAVNE UPRAVE (ODU)

Vlada določi ORGANE DRŽAVNE UPRAVE (ODU) in CSIRT - ODU. CSIRT - ODU ne določi, če imajo ODU v svoji notranji organizacijski strukturi zagotovljene lastne zmogljivosti vsaj na ravni VOC.

VOC je varnostno operativni center, ki se odziva na incidente na področju informacijske varnosti.

ZAVEZANCI SO ODU, ki :

upravljajo z informacijskimi sistemi in deli omrežja oz.

izvajajo informacijske storitve,

nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

OBVEZNOSTI IBS in ODU

- IBS določi **kontaktno osebo** za I.V. + obvesti PNO (ODU le prostovoljno) ;
- **izpolnjevanje varnostnih zahtev- priprava varnostne dokumentacije vključno z ukrepi:** če že imajo (drugi predpisi) – le dopolnijo skladno z ZInfV. Zaradi obvladovanja incidentov: zagotovitev ohranjanje dnevniških zapisov o delovanju ključnih, k. ali n. sistemov oz. delov omrežja (IBS) oz. o delovanju svojih IS ali delov IS (ODU) delov za 6 mesecev (IBS na ozemlju RS, razen za področja digitalna infr., bančništvo in infr. finančnega trga lahko v EU; ODU na ozemlju RS);
- **priglasitev incidentov** s pomembnim vplivom na neprekinjeno izvajanje BS ali storitev ODU. IBS **nacionalnemu CSIRT-u** (ta obvesti še PNO). ODU pa **CSIRT-u ODU** (ta obvesti CSIRT in PNO), **če imajo ODU svoj VOC pa neposredno PNO-ju**. Priglasitelj poskrbi za zavarovanje dnevniških zapisov oz. revizijskih sledi, če obstajajo.

Obveznosti IBS in ODU

VARNOSTNA DOKUMENTACIJA: Dokumentiran sistem upravljanja varovanja informacij in neprekinjenega poslovanja. Obsega najmanj:

1. Analizo obvladovanja tveganj z oceno sprejem. tveganj

2. Politiko neprekinjenega poslovanja

6. NAČRT VARNOSTNIH UKREPOV ZA:

celovitost, zaupnost, razpoložljivost

3. Seznam (IBS ključnih) informacijskih sistemov + delov omrežja s pripadajočimi podatki

4. Načrt obnovitve delovanja

5. Načrt odzivanja na incidente

Pravilnik/a: za IBS in ODU podrobneje določi/ta vsebino/strukturo varnostne dokumentacije z metodologijo ter minimalni obseg in vsebino varnostnih ukrepov (ti so organizacijski, logično-tehnični, tehnični).

OBVEZNOSTI PDS – maksimalna harmonizacija

- **sprejem primernih/ sorazmernih tehničnih in organizacijskih ukrepov za obvladovanje tveganj za zagotovitev varnosti** omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju DS v EU;
- **sprejem ukrepov za preprečitev in zmanjšanje vpliva incidentov** (da bi zagotovili neprekinjeno izvajanje svojih DS v EU);
- **priglasitev incidentov**, ki imajo pomemben vpliv na zagotavljanje DS v EU, **nacionalnemu CSIRT** (ta obvesti še PNO). Obveznost priglasitve je pogojena z dostopom PDS do informacij potrebnih za oceno vpliva;

Pristojnost PNO/ nac. CSIRT, če glavni sedež PDS ali sedež njegovega predstavnika za EU v RS. Prostovoljnost določitve kont. osebe za I.varnost + obvestilo PNO.

+ NEPOSREDNO ZAVEZUJOČA IN UPORABLJIVA IZVEDBENA UREDBA KOMISIJE (EU) 2018/151

http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2018%3A026%3ATOC&uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG

z dodatno specifikacijo elementov pri obvladovanju tveganj za varnost omrežij in informacijskih sistemov, in parametrov za določanje, ali ima incident pomemben vpliv

VREDNOTENJE INCIDENTA/ STANJE POVEČANE OGROŽENOSTI

- priglašene incidente **vrednotijo** nacionalni CSIRT ali CSIRT ODU, če ODU nimajo VOC (sicer neposredno PNO) glede na težo: **lažji, težji ali kritični incident**, lahko gre hkrati tudi za **kibernetski napad** (zakonski kriteriji).
- **stanje povečane ogroženosti** (stanje, ko je podana velika verjetnost realizacije težjega ali kritičnega incidenta oziroma kibernetskega napada v 72 urah od zaznave takšne verjetnosti), razglasi ga **PNO**;
- **PNO z odločbo** (v nujnih primerih lahko tudi ustno) lahko vsem zavezancem naloži **UKREPE** za zaustavitev težjega ali kritičnega incidenta ali kibernetskega napada ali za odpravo posledic, v primeru stanja povečane ogroženosti zaradi preprečitve ali zmanjšanja verjetnosti njegove realizacije pa le za IBS in ODU.
- **PNO obvešča** Vlado in Svet za nacionalno varnost (SNAV) o kritičnem incidentu (lahko o težjem incidentu) in kibernetskem napadu ter o stanju povečane ogroženosti in o sprejetih ukrepih (odločbah).

KIBERNETSKA OBRAMBA

KIBERNETSKA OBRAMBA: celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju.
Usklajujejo in izvajajo jo PNO, oba CSIRT ter MORS, policija, SOVA in drugi pristojni organi pri zagotavljanju nacionalne varnosti. Za ta namen lahko izvajajo usklajene ukrepe/ dejavnosti skladno s svojimi pristojnostmi.

NADZOR

- Nadzor nad izvajanjem določb ZInfV, na njegovi podlagi sprejetih predpisov in nad izvajanjem upravnih odločb (PNO-ja) opravljajo inšpektorji za informacijsko varnost (inšpektor) v okviru PNO;
- Inšpektor obvešča IP, če gre hkrati za kršitev varstva osebnih podatkov ali za sum o tem;
- Inšpekcijski nadzor nad IBS in PDS upoštevajo zahteve iz Direktive NIS (za PDS je blažja ureditev in poudarjeno sodelovanje z drugimi pristojnimi in nadzornimi organi v EU);
- Kazenske določbe: za prekrške se v hitrem postopku sme izreči globa tudi v znesku višjem od najnižje predpisane globe s tem zakonom;

Prehodne določbe - 1

- **Začetek delovanja PNO:** najkasneje do 1. 1. 2020 - do pričetka delovanja PNO njegove naloge opravlja **UVTP** skladno z ZInfV, razen nalog upravnega odločanja in nadzora - te opravlja ministrstvo pristojno za informacijsko družbo (sedaj MJU);
- **Nacionalni CSIRT** začne z delovanjem po tem zakonu 1. 1. 2019;
- **CSIRT ODU** predvidena vzpostavitev na MJU do 1. 1. 2019; do takrat naloge (le) glede obravnave incidentov izvaja nacionalni CSIRT (SI-CERT pri ARNES je incidente namreč že doslej obravnaval);
- **Vlada z ZInfV že uskladila Uredbo o organih v sestavi ministrstev** in umestila Upravo RS za informacijsko varnost (PNO) kot nov organ v sestavi k MJU **ter Sklep o ustanovitvi, nalogah in organizaciji UVTP in** mu do začetka delovanja PNO določila ustrezne naloge (oboje v Uradnem listu RS, št. 52/18),

Prehodne določbe -2

Vlada sprejme Uredbo za določitev seznama BS in podrobnejšo metodologijo za določitev IBS (predvideno je bilo sv 6 mesecih od uveljavitve ZInfV - 11. 11. 2018)

Minister sprejme Pravilnik/a za IBS in ODU s podrobnejšo določitvijo vsebine varnostne dokumentacije, metodologij in varnostnih ukrepov (predvideno je bolo v 6 mesecih od uveljavitve ZInfV - do 11. 11. 2018).

Določitev IBS s strani Vlade: v 6 mesecih od uveljavitve Uredbe za določitev IBS – zgoraj (torej je bilo predvidoma do 11. 5. 2019).

Določitev ODU s strani Vlade: v 9 mesecih od uveljavitve ZInfV (do 11. 2. 2019).

Roki za izpolnjevanje varnostnih zahtev in priglasitve incidentov za zavezance:

- **IBS** v 6. mesecih od njegove določitve za IBS s strani Vlade (– odvisno pa od datuma določitve za IBS);
- **PDS** v 9. mesecih od uveljavitve ZInfV (11. 2. 2019);
- **ODU** v 12. mesecih od njihove določitve s strani Vlade (odvisno pa od datuma določitve ODU).

ZAKLJUČEK

O pripravi podzakonskih aktov je bila in še bo zainteresirana javnost obveščena in povabljena (tudi preko Državnega portala RS, e-uprava, v rubriki E-demokracija, Predlogi predpisov) **k sodelovanju pri pripravi podzakonskih predpisov.**

Javnost je bila tako že povabljena k podaji pripomb in predlogov na osnutek predloga Uredbe o določitvi IBS, ni pa bila še povabljena k podaji pripomb na Pravilnika (zlasti glede IBS), ki sta še v fazi priprave.

HVALA ZA POZORNOST!