Na podlagi četrtega odstavka 16. člena Uredbe o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07 in 86/11) Komisija za informacijsko varnost izdaja

NAVODILO
za povezovanje komunikacijsko informacijskih sistemov, v katerih se obravnavajo tajni podatki

1. člen
(predmet urejanja)

(1) Navodilo predpisuje postopke, pogoje, zahteve in merila, ki jih je potrebno upoštevati pri povezovanju komunikacijsko informacijskih sistemov (v nadaljnjem besedilu: KIS), v katerih se obravnavajo ali hranijo tajni podatki ter odgovornosti in pristojnosti uporabnikov in upraviteljev sistemov.

(2) V primeru povezovanja KIS na mednarodni ravni je potrebno upoštevati tudi navodila, ki se uporabljajo na podlagi mednarodnih pogodb ali sprejetih mednarodnih obveznosti.

(3) To navodilo ne zajema izmenjave informacij z uporabo izmenljivih nosilcev podatkov v elektronski obliki.

2. člen
(pomen izrazov)

Izrazi, uporabljeni v tem navodilu, pomenijo:

- OSI – (Open System Interconnection) referenčni model oziroma nabor internetnih protokolov opredeljenih v ITU-T X.200 standardu,
- SMZ - storitev mejne zaščite (angl. Boundary Protection Service - BPS) je varnostna storitev na vseh OSI nivojih, ki zmanjšuje varnostna tveganja, ki jih prinaša povezovanje KIS. SMZ je praviloma sestavljen iz večjega števila EMZ,
- EMZ – element mejne zaščite (angl. Boundary Protection Component - BPC) na vseh OSI nivojih je programska ali strojna rešitev, ki zagotavlja SMZ. Primeri EMZ so antivirusni program, požarna pregrada, usmerjevalnik, šifrirna naprava, enosmerna podatkovna dioda, itd) in je odobren s strani pristojnega organa,
- Enosmerna podatkovna dioda - tako podatki kot tok podatkov preko tovrstne rešitve potekajo izključno enosmerno (vključno s potrditvenim signalom - »ACK«, ki ga pri tovrstni povezavi ni),
- VPN (angl. Virtual Private Network) - navidezno zasebno omrežje,
- Izjava o skladnosti – izjava upraviteljev sistemov o skladnosti povezave KIS z varnostnimi zahtevami,
- Varnostno dovoljenje za delovanje povezave - potrdilo o izvajanju vseh ukrepov in postopkov za zagotovitev varnega delovanja povezave sistemov,
- Uporabnik je oseba, ki ima v enem od KIS uporabniški račun.

3. člen
(zahteva za povezavo)

(1) Za povezavo dveh ali več KIS je predhodno potreben tehten poslovni ali operativni razlog, ki mora biti pisno opredeljen v Operativni zahtevi za povezavo (v nadaljnjem besedilu: OZP).

(2) V OZP se opredelijo poslovne, operativne in tehnične zahteve, ki vsebujejo:

- razloge za takšno povezavo in pričakovane koristi,
- zahtevo po izmenjavi informacij,
- ravni in načine povezave na vseh OSI nivojih za potrebe opredelitve SMZ in EMZ,
- obstoječo infrastrukturo, relevantno za medsebojno povezovanje
- stopnje tajnosti obravnavanih tajnih podatkov,

- skupnost uporabnikov in
- privilegije uporabnikov.

(3) V OZP (za vsak KIS posebej ali enoten za vse KIS, ki se povezujejo) se posebej opredelijo odgovornosti in pristojnosti upravljavca/ev SMZ.

(4) OZP mora biti pregledana s strani vodij informacijske varnosti in upravljavcev bodočih povezanih sistemov ter odobrena s strani predstojnikov organov ali organizacij.

(5) O vseh spremembah zahtev opredeljenih v OZP je potrebno obvestiti vse ostale upravljavce povezanih KIS. Če pride do sprememb ali novih povezav z drugimi KIS v enem od povezanih sistemov, je potrebno o tem obvestiti upravljavce ostalih povezanih KIS.

4. člen
(načrtovanje povezave)

(1) Ravni in načini povezave na vseh OSI nivojih, ki niso opredeljeni v OZP so prepovedani in jih mora SMZ onemogočati.

(2) Vsak KIS, mora poskrbeti za lastno zaščito nasproti drugemu. Pri tem mora KIS s katerim se povezuje obravnavati kot potencialno varnostno grožnjo.

(3) Za izbiro, namestitev in upravljanje povezovalnih elementov sistema sta odgovorna upravljavca sistema.

(4) Vsaka zahteva, postavljena drugemu KIS, mora biti dokumentirana v izjavi o skladnosti.

(5) Upravljavec je dolžan upravljati in vzdrževati svoj del povezavo tako, da se zagotovi njeno pravilno in varno delovanje.

(6) Upravljavca sta se dolžna med seboj predhodno obveščati o spremembah posameznih KIS, ki bi lahko vplivale na varnostna tveganja ali delovanje povezave. V takih primerih je potrebno obnoviti postopke iz tretjega člena tega navodila.

(7) Varnost pretoka podatkov se zagotavlja s SMZ, ki še zagotavlja najnižje dopustno sprejemljivo tveganje za oba KIS.

(8) Z medsebojno povezavo se lahko namestijo, konfigurirajo in uporabljajo le protokoli, mrežne storitve in toki podatkov, ki so potrebni za izvajanje OZP.

5. člen
(povezovanje KIS)

(1) Povezovanje KIS je dovoljeno le v eni nadzorovani in varovani vstopno-izstopni točki, skozi katero potekajo vsi servisi in storitve.

(2) Povezovanje KIS v katerem obravnavamo tajne podatke z drugim, je dovoljeno le, če je med njiju nameščen SMZ.

(3) SMZ in njegove nastavitve se določijo na podlagi Ocene varnostnih tveganj, da se tveganje zmanjša na najnižjo možno stopnjo.

(4) V KIS, kjer se obravnavajo tajni podatki različnih stopenj tajnosti, mora biti zagotovljeno, da podatki višje stopnje tajnosti ne morejo prehajati v sistem z nižjo stopnjo tajnosti.

(6) Če KIS zagotavlja le komunikacijsko infrastrukturo za prenos tajnih podatkov in so podatki šifrirani s potrjeno šifrirno rešitvijo v skladu z Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, se takšna povezava ne šteje za medsebojno povezavo.

6. člen
(varnostna odobritev povezave)

(1) Predstojniki organov ali organizacij, ki upravljajo posamezne KIS, v katerih se obravnavajo tajni podatki, morajo pred začetkom obratovanja povezav s pisnim sklepom izdati varnostno dovoljenje za delovanje povezave.

(2) Pred izdajo dovoljenja mora predstojnik organa ali organizacije od Urada Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljnjem besedilu: UVTP) pridobiti pozitivno mnenje o varnostni ustreznosti povezave. UVTP-ju se pred izdajo mnenja omogoči varnostni pregled povezave, s katerim preveri izpolnjevanje ukrepov in postopkov za zagotovitev varnega delovanja povezave.

(3) Organ ali organizacija mora o izdaji varnostnega dovoljenja za delovanje povezave obvestiti UVTP.

(4) V primeru, da se KIS povezuje s KIS v katerih se obravnavajo tajni podatki drugih držav ali mednarodnih organizacij, je za izvedbo celotno postopka varnostne odobritve povezave pristojen UVTP, ki tudi izda ustrezno potrdilo.

7. člen
(dokumenti potrebni za izdajo varnostnega dovoljenja za delovanje povezave)

(1) V postopku izdaje varnostnega dovoljenja za povezavo sistemov morajo upravljavci posameznih sistemov, v katerih se obravnavajo tajni podatki pripraviti:

- oceno varnostnih tveganj,
- načrt varovanja povezave z opisom SMZ in EMZ.

V dokumentih morajo biti opisani tudi pogoji pod katerimi se lahko povezava začasno odklopi ali omeji njene storitve ter ukine povezavo.

(2) V okviru dokumentacije je potrebno obravnavati tudi vse že obstoječe povezave med KIS.

8. člen
(povezave med KIS)

(1) Povezave med posameznimi KIS glede na stopnjo tajnosti so:

1. povezovanje KIS istih stopenj tajnosti,
2. povezovanje KIS različnih stopenj tajnosti,
3. povezovanje s KIS brez stopenj tajnosti.

(2) Povezave med dvema KIS velja za medsebojno povezavo, če se sistema razlikujeta najmanj v eni od naslednjih lastnosti:

1. najvišji stopnji obravnavanih tajnih podatkov,
2. varnostnem načinu delovanja,
3. upravitelju KIS in organu za varnostno odobritev KIS,
4. varnostnih zahtevah in veljavni varnostni politiki,
5. drugih varnostnih parametrih (potreba po seznanitvi oz. interesni skupnosti, omejitvah, posebnih protokolih, stopnje fizične zaščite, vrsti nosilnega omrežja, lastništvu podatkov ki se izmenjujejo).

(3) Sprememba KIS, ki pomeni vključitev novih komponent (npr. nova delovna postaja, nova omrežna oprema, itd), ki ne vpliva na katero od lastnosti naštetih v drugem odstavku tega člena, ne velja za medsebojno povezavo.

(4) V primeru nejasnosti, ali povezava med posameznimi KIS predstavlja medsebojno povezavo dveh KIS ali ne, odloča pristojni nacionalni varnostni organ (organ za varnostne odobritve KIS).

9. člen
(Modeli medsebojne povezave)

(1) Medsebojno povezavo KIS opisujeta dva parametra:
- varnostni pogoji, ki so sklop lastnosti opredeljenih v drugem odstavku osmega člena tega navodila in
- vloge, ki opisuje vlogo KIS v medsebojni povezavi.

(2) Vloge KIS v medsebojni povezavi opredeljujejo:
- smer toka podatkov s stališča KIS in
- zagotavljanje storitev, vloga KIS v zagotavljanju ali uporabi storitev, ki jo zagotavlja medsebojna storitev.

(3) Vrednosti vloge iz posamezne lastnosti iz prejšnjega odstavka so podane v spodnji preglednici.

Lastnost	Vrednost	Opis
smer toka	Prejemanje	KIS prejema podatke iz drugega KIS
	Pošiljanje	KIS pošilja podatke drugemu KIS
	Pošiljanje/Prejemanje	KIS pošilja in prejema podatke
zagotavljanje storitev	Uporaba (uporabnik storitev)	KIS uporablja storitve, ki jih zagotavlja drugi KIS - odjemalec
	Zagotavljanje (ponudnik storitev)	KIS zagotavlja storitve za drugi KIS - strežnik
	Uporaba/Zagotavljanje	KIS zagotavlja storitve drugemu KIS in uporablja njegove storitve

(4) Vrednosti vlog iz prejšnjega odstavka je potrebno natančno opredeliti v OPZ.

(5) Pogoji glede določanja toka ali storitev iz prvega odstavka 8.člena.

	določitev toka podatkov ali storitev	Dovoljeno	izjema
Povezovanje KIS istih stopenj tajnosti	Vsak tok ali storitev iz OZP mora biti natančno določena		
Povezovanje KIS različnih stopenj tajnosti.	Vsak tok ali storitev iz OZP mora biti natančno določena	Dovoljen samo enosmerni tok iz KIS nižje stopnje tajnosti v KIS za višjo stopnjo tajnosti	Podatkovni tok iz KIS višje stopnje tajnosti v KIS nižje stopnje tajnosti, samo pod pogojem, da so podatki natančno varnostno označeni (labelirani) in se na EMZ/SMZ izvaja nadzor pretoka podatkov.
Povezovanje s KIS brez stopnje tajnosti.	Vsak tok ali storitev iz OZP mora biti natančno določena	KIS z najvišjo stopnjo tajnosti podatkov za kontrolirano dvosmerno povezovanje je INTERNO	KIS za višje stopnje tajnosti se lahko z internetom povezujejo samo enosmerno iz interneta oziroma KIS nižje stopnje tajnosti v KIS z višjo stopnjo tajnosti. Pri tovrstnem načinu je obvezna uporaba enosmerne podatkovne diode.

10. člen
(izvedbena navodila)

(1) Do sprejetja ustreznih nacionalnih tehničnih navodil se uporabljajo dokumenti mednarodnih organizacij, v katerih je Republika Slovenija polnopravna članica. Komisija za informacijsko varnost s sklepom določi seznam veljavnih tehničnih navodil za povezovanje KIS.

(2) Za povezovanje KIS organov z mednarodnimi organizacijami in KIS mednarodnih operacij se uporablja za to relevantna dokumentacija mednarodnih organizacij (npr. NATO in EU).

(3) Pred povezavo KIS organov s KIS tujih organizacij mora biti sklenjen ustrezen varnostni sporazum - bilateralni sporazum o izmenjavi in medsebojnem varovanju tajnih podatkov, med organoma za komunikacijsko varnost mora biti dosežen dogovor o uporabi šifrirne opreme, oba KIS pa morata imeti veljavno varnostno dovoljenje za delovanje sistema.

(4) Pri uporabi izvedbenih navodil in dokumentov iz prvega odstavka tega člena, je potrebno zagotoviti:

- dostop do teh navodil samo tistim, ki jih nujno potrebujejo za izvajanje svoje naloge po principu »potrebe po vedenju«,
- uporabniki ali prejemniki navodil morajo imeti ustrezno dovoljenje za dostop do tajnih podatkov,
- primerno varovanje dokumentov.

11. člen
(varovanje naprav)

EMZ so ključne sestavine KIS, ki morajo biti postavljene v prostor varovan najmanj tako, kot je določeno v Uredbi o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11 in 24/11 – popr.) za najvišjo stopnjo tajnosti obravnavanih podatkov.

12. člen
(dostop in nadzor izmenjave podatkov)

(1) Nadzorni mehanizmi morajo biti taki, da se dostop do tajnih podatkov omogoči samo uporabnikom, ki imajo ustrezno dovoljenje za dostop do tajnih podatkov in se morajo s tajnimi podatki seznaniti zaradi opravljanje funkcije ali delovnih nalog. Dostop do KIS storitev in podatkov je dovoljen samo na podlagi odobritve.

(2) Izmenjava podatkov med KIS je dovoljena le s strani upravljavcev pooblaščenim uporabnikom oziroma procesom.

(3) Nadzor nad izmenjavo izvršljivih datotek (npr. makro, JavaScript, ActiveX controls, itd) se izvaja v skladu z načrtom varovanja sistema.

(4) Skladno z Oceno tveganja se uporabijo primerni mehanizmi za zaznavanje in preprečevanje zlonamernih aktivnosti skozi SMZ (nenadzorovan pretok podatkov, pretok zlonamerne kode, zaznavanje nepredvidenih aktivnosti, itd).

13. člen
(evidenca povezav)

UVTP vodi evidenco vseh povezav KIS, za katere je izdano varnostno dovoljenje za delovanje povezave.

14. člen
(prehodno obdobje)

Za že povezane KIS je potrebno varnostno dovoljenje za delovanje povezave pridobiti v roku dveh let od sprejetja tega navodila.

15. člen
(veljavnost)

Navodilo prične veljati naslednji dan po podpisu.

Igor Eršte
Predsednik Komisije za informacijsko varnost

Številka: 012-3/2019/10
Datum: 22. 2. 2019