

Priloga 9: Postopki in merila za povezovanje komunikacijsko informacijskih sistemov, v katerih se varujejo tajni podatki

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

Ti postopki in merila ne zajemajo izmenjave informacij z uporabo izmenljivih elektronskih nosilcev podatkov.

Pomen izrazov uporabljenih v tej prilogi

Izrazi, uporabljeni v tej prilogi, 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 sistemov. 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 sistemov 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 sistemov uporabniški račun.

Zahteva za povezavo

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

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 varovanih tajnih podatkov,
- skupnost uporabnikov in
- privilegije uporabnikov.

V OZP (za vsak sistem posebej ali enoten za vse sisteme, ki se povezujejo) se posebej opredelijo odgovornosti in pristojnosti upravljavca SMZ.

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

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

Načrtovanje povezave

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

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

Za izbiro, namestitve in upravljanje povezovalnih elementov posameznega sistema sta odgovorna upravljavca sistemov.

Vsaka zahteva, postavljena drugemu sistemu, mora biti dokumentirana v izjavi o skladnosti.

Upravljavca je dolžan upravljati in vzdrževati svoj del povezavo tako, da se zagotovi njeno pravilno in varno delovanje.

Upravljavca sta se dolžna med seboj predhodno obveščati o spremembah posameznih sistemov, ki bi lahko vplivale na varnostna tveganja ali delovanje povezave. V takih primerih je potrebno obnoviti postopke iz prejšnjega poglavja. Zahteva za povezavo te priloge.

Varnost pretoka podatkov se zagotavlja s SMZ, ki še zagotavlja najnižje dopustno sprejemljivo tveganje za povezane sisteme.

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

Povezovanje sistemov

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

Povezovanje sistemov v katerem varujemo tajne podatke z drugim, je dovoljeno le, če je med njiju nameščen SMZ.

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

V sistemu, kjer se varujejo tajni podatki različnih stopenj tajnosti, mora biti zagotovljeno, da podatki višje stopnje tajnosti ne morejo prehajati v sistem z nižjo stopnjo tajnosti.

Če sistem zagotavlja le komunikacijsko infrastrukturo za prenos tajnih podatkov in so podatki kriptirani s kriptografsko rešitvijo za katero je bilo izdano potrdilo o varnostni ustreznosti v skladu s to uredbo, se takšna povezava ne šteje za medsebojno povezavo.

V postopku izdaje varnostnega dovoljenja za povezavo sistemov morajo upravljavci posameznih sistemov, v katerih se varujejo 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.

V okviru dokumentacije je potrebno obravnavati tudi vse že obstoječe povezave med sistemi.

Povezave med sistemi

Povezave med posameznimi sistemi glede na stopnjo tajnosti so:

- sistemi, ki se povezujejo so istih stopenj tajnosti,
- sistemi, ki se povezujejo so različnih stopenj tajnosti,
- sistemi, brez stopenj tajnosti se povezujejo s sistemi s stopnjami tajnosti.

O medsebojni povezavi sistemov, govorimo, v primerih, ko se sistema razlikujeta najmanj v eni od naslednjih lastnosti:

- najvišji stopnji varovanih tajnih podatkov,

- varnostnem načinu delovanja,
- upravitelju sistema in organu za varnostno odobritev sistema,
- varnostnih zahtevah in veljavni varnostni politiki,
- drugih varnostnih parametroh (potreba po seznanitvi oz. interesni skupnosti, omejitvah, posebnih protokolih, stopnje fizične zaščite, vrsti nosilnega omrežja, lastništvu podatkov ki se izmenjujejo).

Dodajanje novih komponent (npr. nova delovna postaja, nova omrežna oprema, itd.), obstoječemu sistemu, ki hkrati ne vplivajo na katero od lastnosti naštetih v prejšnjem odstavku, se ne štejejo kot povezovanje sistemov.

Modeli medsebojne povezave

Medsebojno povezavo sistemov opisujeta dva parametra:

- varnostni pogoji, ki se določajo na podlagi lastnosti, ki opredeljujejo medsebojno povezavo dveh sistemov in
- vloge, ki opisuje vlogo sistema v medsebojni povezavi.

Vloge sistemov v medsebojni povezavi opredeljujejo:

- smer toka podatkov s stališča sistema in
- zagotavljanje storitev, vloga sistema v zagotavljanju ali uporabi storitev, ki jo zagotavlja medsebojna storitev.

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

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

Vrednosti vlog iz prejšnjega odstavka je potrebno natančno opredeliti v OZP.

Pogoji glede določanja toka ali storitev.

	določitev toka podatkov ali storitev	Dovoljeno	izjema
Povezovanje sistemov istih stopenj tajnosti	Vsak tok ali storitev iz OZP mora biti natančno določena		
Povezovanje sistemov različnih stopenj tajnosti.	Vsak tok ali storitev iz OZP mora biti natančno določena	Dovoljen samo enosmerni tok iz sistema nižje stopnje tajnosti v sistem za višjo stopnjo tajnosti	Podatkovni tok iz sistema višje stopnje tajnosti v sistem nižje stopnje tajnosti, samo pod pogojem, da so podatki natančno varnostno označeni (labelirani) in se na EMZ/SMZ izvaja nadzor pretoka podatkov.
Povezovanje s sistemom brez stopnje tajnosti.	Vsak tok ali storitev iz OZP mora biti natančno določena	Sistem z najvišjo stopnjo tajnosti podatkov za kontrolirano	Sistem za višje stopnje tajnosti se lahko z internetom povezujejo samo enosmerno iz interneta oziroma sistema nižje stopnje

		dvosmerno povezovanje je INTERNO	tajnosti v sistem z višjo stopnjo tajnosti. Pri tovrstnem načinu je obvezna uporaba enosmerne podatkovne diode.
--	--	--	--

Dostop in nadzor izmenjave podatkov

Nadzorni mehanizmi povezanih sistemov 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.

Izmenjava podatkov med povezanimi sistemi je dovoljena pooblaščenim uporabnikom ali odobrenim procesom.

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

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).