Priloga 10: Postopki in merila za povezovanje sistemov

Pri povezovanju sistemov na mednarodni ravni se upoštevajo 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) je referenčni model oziroma nabor internetnih protokolov, opredeljenih v standardu ITU-T X.200;
- SMZ – storitev mejne zaščite (angl. Boundary Protection Service – BPS) je varnostna storitev na vseh OSI plasteh, ki zmanjšuje varnostna tveganja zaradi povezovanja sistemov. SMZ je praviloma sestavljen iz večjega števila EMZ;
- EMZ – prvina mejne zaščite (angl. Boundary Protection Component – BPC) na vseh OSI plasteh je programska ali strojna rešitev, ki zagotavlja SMZ. Primeri EMZ, ki ga je odobril pristojni organ, so antivirusni program, požarna pregrada, usmerjevalnik, kriptografska rešitev, enosmerna podatkovna dioda in podobni;
- enosmerna podatkovna dioda – tako podatki kot tok podatkov prek te rešitve potekajo izključno enosmerno (vključno s potrditvenim signalom ACK, ki ga pri tej 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 plasteh za potrebe opredelitve SMZ in EMZ,
- obstoječo infrastrukturo, pomembno 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 prihodnjih povezanih sistemov ter odobrena s strani predstojnikov organov ali organizacij.

O vseh spremembah zahtev, opredeljenih v OZP, je treba obvestiti vse preostale upravljavce povezanih sistemov. Če pride do sprememb ali novih povezav z drugimi sistemi v enem od povezanih sistemov, je treba o tem obvestiti upravljavce preostalih povezanih sistemov.

Načrtovanje povezave

Ravni in načini povezave na vseh OSI plasteh, ki niso opredeljeni v OZP, niso dovoljeni in jih mora SMZ onemogočati.

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

Za izbiro, namestitev in upravljanje povezovalnih prvin posameznega sistema sta odgovorna upravljavca sistemov.

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

Upravljavec mora upravljati in vzdrževati svoj del povezave tako, da se zagotovi njeno pravilno in varno delovanje.

Upravljavca se morata med seboj predhodno obveščati o spremembah posameznih sistemov, ki bi lahko vplivale na varnostna tveganja ali delovanje povezave. V takih primerih je treba obnoviti postopke iz operativnih zahtev za povezavo.

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, 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 se varujejo tajni podatki, z drugim sistemom, je dovoljeno le, če je mednju 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 potrdilom 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 se omejijo njene storitve ter ukine povezava.

V okviru dokumentacije je treba obravnavati tudi vse že vzpostavljene povezave med sistemi.

Povezave med sistemi

Povezave med posameznimi sistemi glede na stopnjo tajnosti:
- 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:
- najvišja stopnja varovanih tajnih podatkov,
- varnostni način delovanja,

– upravitelj sistema in organ za varnostno odobritev sistema,
– varnostne zahteve in veljavna varnostna politika,
– drugi varnostni parametri (potreba po seznanitvi oz. interesni skupnosti, omejitve, posebni protokoli, stopnja fizične zaščite, vrsta nosilnega omrežja, lastništvo podatkov, ki se izmenjujejo).

Dodajanje novih komponent (npr. nova delovna postaja, nova omrežna oprema) že vzpostavljenemu 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 in opredeljujejo medsebojno povezavo dveh sistemov, ter
– vloge, ki opisujejo vlogo sistema v medsebojni povezavi.

Vloge sistemov v medsebojni povezavi opredeljujejo:
– smer toka podatkov s stališča sistema in
– zagotavljanje storitev, vlogo 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 podatkov	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 treba natančno opredeliti v OPZ.

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 je 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 dvosmerno	Sistemi za višje stopnje tajnosti se lahko z medomrežjem (internetom) povezujejo samo enosmerno iz medomrežja oziroma sistema nižje stopnje

		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 opravljanja 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) se izvaja v skladu z načrtom varovanja sistema.

Skladno z oceno tveganja se uporabijo primerni mehanizmi za zaznavanje in preprečevanje zlonamernih aktivnosti prek SMZ (nenadzorovan pretok podatkov, pretok zlonamerne kode, zaznavanje nepredvidenih aktivnosti itn.).