



APEK

**Agencija za pošto in elektronske
komunikacije Republike Slovenije**
Stegne 7, p. p. 418
1001 Ljubljana
telefon: 01 583 63 00, faks: 01 511 11 01
e-naslov: info.box@apek.si, <http://www.apek.si>
davčna št.: 10482369

Izdaja: V1.0 z dne 01.09.2006

Smernice za zagotavljanje varnosti omrežij elektronskih komunikacij in informacijskih sistemov

Vsebina

1.	Uvod	3
1.1.	Namen smernic	3
1.2.	Pomen smernic.....	3
1.3.	Izhodišča za smernice	3
1.4.	Izrazi in definicije	4
1.5.	Standardizacija	4
1.6.	Reference	5
2.	Smernice	6

1. Uvod

1.1. Namen smernic

Zakon o elektronskih komunikacijah [1] v poglavju o zaščiti tajnosti in zaupnosti elektronskih komunikacij vsebuje zahtevo, da operaterji vsak zase ali po potrebi skupaj sprejmejo ustrezne tehnične in organizacijske ukrepe, da zagotovijo varnost svojega omrežja oziroma svojih storitev. Strategija za varno informacijsko družbo [2] postavlja zagotavljanje varnosti omrežij in informacijskih sistemov kot ključni izziv, saj ima lahko kršitev varnostnih zahtev vpliv, ki presega gospodarske dimenzije. Obstaja splošna zaskrbljenost, da bo pomanjkljiva varnost omrežij in storitev ustvarjala negativno uporabniško izkušnjo in bo odvrčala uporabnike od masovne uporabe storitev informacijske družbe. Zagotavljanje varnih in zanesljivih omrežij in informacijskih sistemov so bistvenega pomena tudi za delovanje drugih ključnih infrastruktur, kot so promet, energija itd.

Skratka, varnost omrežij in informacijskih sistemov je bistvenega pomena tako za razvoj slovenskega gospodarstva in družbenega sistema kakor za vzpostavitev enotnega evropskega informacijskega prostora.

Namen smernic za zagotavljanje varnosti omrežij elektronskih komunikacij in informacijskih sistemov je:

- nudenje skupne podlage za uvajanje in merjenje učinkovitosti metod varovanja informacij,
- natančna navedba varnostnih standardov in priporočil za zagotavljanje osnovne ravni varovanja informacij in poslovne kontinuitete,
- zagotavljanje primernih in sorazmernih varnostnih ukrepov, ki bodo krepili zaupanje uporabnikov v varnost storitev informacijske družbe.

Te smernice imajo status priporočila in veljajo predvsem za javna komunikacijska omrežja in informacijske sisteme.

1.2. Pomen smernic

Agencija za pošto in elektronske komunikacije (v nadaljevanju: agencija) šteje smernice za zagotavljanje varnost omrežij elektronskih komunikacij in informacijskih sistemov, kot dobro prakso za varovanje informacij v javnih komunikacijskih omrežjih in informacijskih sistemih.

Ta dokument se objavlja v obliki smernic. Preverjanja skladnosti s temi smernicami agencija ne bo opravljala.

Če se bo izkazala potreba, se lahko v tem dokumentu vsebovana priporočila spremenijo tudi v ustrezne podzakonske akte.

1.3. Izhodišča za smernice

Agencija je pri izdelavi tega dokumenta upoštevala rezultate dela tehničnih odborov za standardizacijo, strategijo EU za varno informacijsko družbo [2], priporočila neodvisne regulatorne skupine (IRG) za varnost informacij, prakso drugih neodvisnih regulatornih organov [3] in interese končnih uporabnikov storitev elektronskih komunikacij.

1.4. Izrazi in definicije

Varnost omrežij in informacijskih sistemov (Network and information System Security) je zmožnost omrežja ali informacijskega sistema, da z določeno stopnjo gotovosti prepreči naključne dogodke ali zlonamerna dejanja, ki ogrožajo zaupnost, verodostojnost, celovitost ali razpoložljivost shranjenih ali prenesenih podatkov ter s tem povezanih storitev, ki jih ponujajo ta omrežja in sistemi ali so prek njih dostopne.

Sistem za upravljanje varovanja informacij (Information Security Management System) je tisti del celotnega sistema upravljanja, ki temelji na pristopu poslovnega tveganja in zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varovanja informacij. Sistem za upravljanje vključuje strukturo organizacije, politike, dejavnost načrtovanja, odgovornosti, splošne rabe, postopke, procese in sredstva.

Načrt za neprekinjeno poslovanje (Business Continuity Plan) je dokumentirana zbirka postopkov in navodil, ki se redno posodablja in vzdržuje z namenom nemotenega zagotavljanja sredstev in storitev v primeru incidentov.

Načrt za ponovno vzpostavitev (Disaster Recovery Plan) je dokumentirana zbirka postopkov in navodil, ki se redno posodablja in vzdržuje z namenom ponovne vzpostavitve vseh kritičnih okolij omrežja ali informacijskega sistema, ko se zgodi incident.

Incident (Incident) je eden ali več neželenih dogodkov, za katere je zelo verjetno, da bodo ogrozili poslovanje organizacije. Za incidente se štejejo naravne katastrofe, vojna ali izredna stanja, izpadi električne energije, teroristična dejanja, zlonamerna dejanja posameznikov ali organizacij, okvare na elementih omrežja oziroma informacijskega sistema, človeške napake, delavske stavke itd.

Sredstvo (Asset) je vse, kar ima določeno vrednost za organizacijo.

Politika (Policy) je splošen namen in usmeritev, kot ju uradno izrazi vodstvo podjetja.

1.5. Standardizacija

Standard SIST ISO/IEC 27001:2006 in priporočilo ITU-T X.1051 podajata metodo, ki omogoča izdelavo, uresničitev, obvladovanje in stalne izboljšave sistema za upravljanje varovanja informacij. Standard SIST ISO/IEC 27001:2006 in priporočilo ITU-T X.1051 uporabljajo tako zaposleni neke organizacije kot tudi pooblaščenici zunanji ocenjevalci. Na ta način lahko neodvisna ocena akreditiranega certifikacijskega organa privede do priznanega ovrednotenja, ki dokazuje, da omenjeno podjetje obvlada upravljanje varovanja informacij.

Priporočilo mednarodne zveze za telekomunikacije ITU-T X.1051 sledi standardu BS 7799-2:2002, ki je bil v letu 2005 revidiran in objavljen kot mednarodni standard ISO/IEC 27001:2005 (SIST ISO/IEC 27001:2006).

Struktura in metodologija standarda SIST ISO/IEC 27001:2006 sta dosledno usklajena s standardi za sisteme vodenja SIST EN ISO 9001:2000 in SIST EN ISO 14001:2004, tako da je z ustreznimi oblikovanim celovitim sistemom za upravljanje možno pregledno izpolniti zahteve vseh teh standardov. V tabeli C.1 standada SIST ISO/IEC 27001:2006 je prikazano medsebojno razmerje in povezanost omenjenih standardov. Standardi SIST ISO/IEC 27001:2006, SIST EN ISO 9001:2000 in SIST EN ISO 14001:2004 so splošne narave in so namenjeni vsem organizacijam, ne glede na njihovo velikost ali dejavnost.

Standard SIST ISO/IEC 27001:2006 spodbuja privzem procesnega pristopa in načelo nenehnih izboljšav. Procesni pristop zagotavlja nenehni nadzor nad povezavami posameznih procesov, njihovimi kombinacijami, medsebojnimi vplivi in zaporedji. Načelo nenehnih izboljšav pa zagotavlja nenehno izboljševanje procesov na osnovi objektivnih merjenj. Načelo nenehnih izboljšav ima štiri

faze, in sicer »Načrtuj-Izvedi-Preveri-Ukrepaj« (*Plan-Do-Check-Act*), ki se ponavljajo v rednih časovnih presledkih.

V prvi fazi (načrtuj) se vzpostavi okvir upravljanja varovanja informacij. Vključuje določanje ciljev, identifikacijo procesov, identifikacijo in oceno tveganj, definiranje varnostne politike, planiranje človeških in finančnih virov za uresničevanje zastavljenih ciljev itd. Če se organizacija ravna po standardu SIST ISO/IEC 17799:2006, mora med drugim izbrati postopke, kontrole in cilje kontrol, ki ustrezajo definirani politiki in tveganjem, pred katerimi se želi zaščititi. Izbor se zapiše v izjavo o uporabnosti (*Statement of Applicability*), ki jo potrdi vodstvo podjetja kot dokaz, da se strinja s postopki, kontrolnimi cilji in neupoštevanimi preostalimi tveganji. Druga faza (*izvedi*) je usmerjena na izvedbo načrtovanih postopkov in kontrol. V naslednji fazi (*preveri*) se izvaja analiza sposobnosti sistema za doseganje zastavljenih ciljev, analiza implementacije postopkov v praksi, poročanje o dobljenih rezultatih itd. Ta analiza mora upoštevati tudi trenutno stopnjo razvoja tehnologije, organizacijske spremembe in pravno okolje. Ponovno je potrebno oceniti tudi neupoštevana preostala tveganja, kot tudi vsa ostala dejanska stanja, ki so bila opredeljena in bi lahko vplivala na učinkovitost sistema za upravljanje varovanja informacij. V zadnji fazi (*ukrepaj*) je predvidena uporaba korektivnih in preventivnih ukrepov, ki so osnovani na izidih analiz, ki so bile opravljene v tretji fazi (*preveri*). Nujno je, da se vse štiri omenjene faze redno izvajajo, da se zagotovijo stalne izboljšave sistema upravljanja varovanja informacij in s tem njegova zanesljivost.

1.6. Reference

- [1] Zakon o elektronskih komunikacijah (Ur. l. RS št. 43/2004);
- [2] Sporočilo komisije svetu, evropskemu parlamentu, ekonomsko-socialnemu odboru in odboru regij: Strategija za varno informacijsko družbo-»Dialog, partnerstvo ter povečanje vpliva in moči«, SEC(2006)656;
- [3] Smernice za varnost in razpoložljivost telekomunikacijskih struktur in storitev, izdaja: 1, 28.04.2006 (Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und –diensten), OFCOM Federal Office of Communications, Švica;
- [4] SIST ISO/IEC 27001:2006 Informacijska tehnologija - Varnostne tehnike - Sistem za upravljanje varovanja informacij;
- [5] SIST ISO/IEC 17799:2005 Informacijska tehnologija - Varnostne tehnike - Kodeks za upravljanje varovanja informacij;
- [6] ITU-T X.1051 (07/2004) Sistem za upravljanje varovanja informacij - Zahteve za telekomunikacije (ISMS-T).

2. Smernice

1. Vsak operater mora dokumentirati, vzpostaviti, vzdrževati, nadzorovati in nenehno izboljševati sistem za upravljanje varovanja informacij, kot je to opisano v naslednjih dokumentih:
 - a. Standardi SIST ISO/IEC 27001:2006 [4] in SIST ISO/IEC 17799:2005 [5] ali
 - b. Priporočilo ITU-T X.1051 [6].
2. Vsak operater mora izdelati načrt za neprekinjeno poslovanje (Business Continuity Plan) in načrt za ponovno vzpostavitev (Disaster Recovery Plan), ki sta osnovana na varnostni politiki in sistemu za upravljanje varovanja informacij ter ju dokumentirati, vzpostaviti, vzdrževati, nadzorovati in nenehno izboljševati.
3. Vsak operater se mora prepričati, ali njihovi postopki in infrastruktura ustrezajo zahtevam teh smernic.



mag. Tomaž Simonič
direktor