REVIZIJA INFORMACIJSKEGA SISTEMA NA PRIMERU VARSTVA OSEBNIH PODATKOV

Urška Kežmah[*], *Boštjan Kežmah*[**]

UDK: 342.7:004

***Urška Kežmah, Boštjan Kežmah: Revizija informacijskega sistema na primeru varstva osebnih podatkov**. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Zbornik referatov z dopolnilnega izobraževanja, Maribor 6/2007, str. 63-69.*

Izvirnik v slovenščini, izvleček v slovenščini in angleščini, povzetek v angleščini.

Prispevek obravnava potek revizije informacijskega sistema ter njegovo svetovalno vlogo za ravnateljstvo in upravitelje informacijskega sistema in identificira nekatere probleme v zvezi z zbiranjem in varovanjem osebnih podatkov.

UDC: 342.7:004

***Urška Kežmah, Boštjan Kežmah: Information System Auditing in the Case of Personal Data Protection**. Technical and Field Related Problems of Traditional and Electronic Archiving. Conference Proceedings, Maribor 6/2007, pp. 63-69.*

Original in Slovenian, abstract in Slovenian and English, summary in English.

The article discusses information system auditing and its advising role for the management and governance of the information system and identifies some problems concerning collection and protection of personal data.

UVOD

Revizija informacijskega sistema je v osnovi pregled kontrol, vzpostavljenih v informacijskem sistemu revidirane enote. Izvedena je lahko v kombinaciji z revizijo računovodskih izkazov, interno revizijo ali drugo obliko preizkušanja in/ali ocenjevanja. Revizor v postopku revizije pridobiva, pregleduje, analizira in presoja podatke o informacijskem sistemu, večinoma z namenom, da si o informacijskem sistemu pridobi neodvisno strokovno mnenje, ki ga zapiše v obliki poročila o reviziji.

ZAKONSKA PODLAGA ZA REVIZIJO

Revidiranje v prvi vrsti opredeljuje Zakon o revidiranju (ZRev-1[1]). Čeprav se v osnovi nanaša na revidiranje računovodskih izkazov, v 2. členu opredeljuje, da mora revidiranje potekati na način, določen s tem zakonom, temeljnimi revizijskimi načeli in drugimi pravili revidiranja, ki jih sprejema Slovenski inštitut za revizijo (v nadaljnjem besedilu: inštitut) ter mednarodnimi standardi revidiranja in mednarodnimi stališči o revidiranju, ki jih pri Mednarodnem združenju računovodij sprejema Mednarodni odbor za pravila revidiranja, in drugimi zakoni, ki urejajo

[*] ***Mag. Urška Kežmah, Univerza v Mariboru, Pravna fakulteta, Mladinska ulica 9, 2000 Maribor, Slovenija.***

[**] ***Mag. Boštjan Kežmah, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, Smetanova ulica 17, 2000 Maribor, Slovenija.***

[1] *Ur.l. RS, št. 11/2001, 118/2005 Odl.US: U-I-219/03-25, 42/2006-ZGD-1 (60/2006 - popr.).*

revidiranje posameznih pravnih oseb oziroma druge oblike revizije, in predpisi, izdanimi na njihovi podlagi (v nadaljnjem besedilu: pravila revidiranja).

Po 2. členu ZRev-1 se torej tudi za »druge oblike revizije« kot krovni zakon uporablja ZRev-1, kar velja tudi za revizijo informacijskih sistemov, ki je v 5. čl. ZRev-1 opredeljena kot eno izmed strokovnih področij, povezanih z revidiranjem:

- računovodstvo,
- poslovne finance,
- notranje revidiranje,
- revidiranje informacijskih sistemov,
- davčno proučevanje in svetovanje,
- ocenjevanje vrednosti podjetij, nepremičnin ter strojev in opreme.

V nasprotju s splošnim prepričanjem se revidiranje informacijskega sistema ne opravlja samo v primerih, določenih z zakonom, temveč ga periodično naroča skrbno poslovodstvo, da se prepriča o učinkoviti, uspešni in varni uporabi, izrabi ter upravljanju informacijskega sistema. Izvajanje revidiranja po naročilu podjetja izrecno dovoljuje tudi 2. odst. 2. člena ZRev-1.

SLOVENSKI INŠTITUT ZA REVIZIJO

Slovenski inštitut za revizijo je pravna oseba, za katero se uporabljajo določbe Zakona o zavodih, če ni z ZRev-1 drugače določeno. Ustanovitelj je Zveza računovodij, finančnikov in revizorjev Slovenije.

Opravlja naloge in pristojnosti s področja revidiranja in drugih strokovnih področjih, povezanih z revidiranjem, kot smo navedli zgoraj.

Po 1. tč. 2. odst. 12. čl. ZRev-1 Inštitut sprejema in objavlja naslednje strokovne standarde:

- računovodske standarde,
- standarde revidiranja,
- poslovnofinančne standarde,
- standarde notranjega revidiranja,
- standarde revidiranja informacijskih sistemov,
- standarde na področju ocenjevanja vrednosti podjetij, nepremičnin ter strojev in opreme.

Povedano drugače je Inštitut pristojen za sprejem in objavo standardov za vsa v ZRev-1 navedena strokovna področja, povezana z revidiranjem.

Razen standardov po 5. tč. 2. odst. 12. čl. ZRev-1 določa strokovna znanja in izkušnje, potrebne za pridobitev naslednjih strokovnih nazivov:

- preizkušeni notranji revizor,
- preizkušeni računovodja,
- preizkušeni poslovni finančnik,

- preizkušeni revizor informacijskih sistemov,

in po 6. tč. 2. odst. 12. čl. ZRev-1 organizira strokovno izobraževanje, izvaja preizkuse strokovnih znanj in izdaja potrdila o strokovnih znanjih za pridobitev strokovnih nazivov.

Osebe, ki jim Inštitut podeli strokovni naziv, so vpisane v register, ki ga v skladu z 8. tč. 2. odst. 12. čl. ZRev-1 vodi Inštitut.

Register je dostopen tudi na internetu v okviru spletnih strani Inštituta (http://www.si-revizija.si). Seznam preizkušenih revizorjev informacijskih sistemov, ki izpolnjujejo pogoje za objavo, je npr. dostopen na spletnem naslovu http://www.si-revizija.si/revizorji_is/register-reviz_is.html. Kot zanimivost zapišimo, da je na seznamu dne 3. 2. 2007 navedenih 26 preizkušenih revizorjev informacijskih sistemov.

PROCES REVIDIRANJA INFORMACIJSKIH SISTEMOV

Ker ni splošno priznane definicije revizije informacijskih sistemov, bomo uporabili definicijo, kot jo je predstavil Ron Weber[1]. Revizija je proces zbiranja in presojanja dokazov za ugotavljanje, ali računalniški sistem (informacijski sistem) varuje premoženje, vzdržuje integriteto podatkov, učinkovito dosega cilje organizacije in učinkovito porablja vire.

Sodobni informacijski sistemi niso namenjeni izključno shranjevanju podatkov, temveč poganjajo ključne poslovne procese. Zaradi tega vodstvo in poslovodstvo primerno skrbi za informacijski sistem. Namen revizije informacijskega sistema je nuditi podporo vodstvu in poslovodstvu pri ključnih odločitvah s preiskovanjem in podajanjem povratne informacije, zagotovil ter priporočil. Pomembnejši vidiki informacijskega sistema, ki jih naslovi revizija, so:

- **Dostopnost**. Ali bo informacijski sistem, na katerem temeljijo ključni poslovni procesi, ves čas na voljo? Ali so sistemi primerno zaščiteni v primeru izgub in katastrof?
- **Zaupnost**. Ali bo informacija, shranjena v sistemu, predstavljena le tistemu, ki mora imeti dostop do informacije?
- **Integriteta**. Ali bodo dostopne informacije vedno točne, zanesljive in ažurne? Kaj zagotavlja, da ni možno narediti nobene nepooblaščene spremembe v podatkih ali programski opremi?

Razen teh temeljnih vidikov revidiranje ugotavlja tudi učinkovitost, uspešnost, vrednost informacijskega sistema, povračilo investicije, odgovarja na vprašanja, povezana z ljudmi in kulturo.

KOMPONENTE INFORMACIJSKEGA SISTEMA IN NJEGOVE REVIZIJE

Informacijski sistem ni le računalnik. Sodobni informacijski sistemi so zapleteni in so sestavljeni iz večjega števila komponent, ki kot celota tvorijo poslovno rešitev. Zagotovila o informacijskem sistemu je možno pridobiti le s preverjanjem vseh komponent. Pomembnejše elemente revizije informacijskega sistema lahko strnemo v naslednje točke:

Fizični pregled in pregled okolja. Vključuje fizično varovanje, napajanje z energijo, prezračevanje, nadzor nad vlažnostjo in druge vplive okolja.

1. Pregled administracije sistema. Se nanaša na varnostni pregled operacijskih sistemov, sistemov za upravljanje s podatki, postopkov za administracijo sistema in skladnost.
2. Pregled uporabniške programske opreme. Poslovna aplikacija je lahko izračun plač, izdajanje računov, sistem za spletno sprejemanje naročil ali celoviti informacijski sistem, ki dejansko poganja poslovanje. Pregled vključuje kontrolo dostopa in avtorizacij, validacijo, upravljanje z napakami in izjemami, tok poslovnih procesov v uporabniški programski opremi ter spremljajoče ročne kontrole in postopke. Sem spada tudi pregled življenjskega cikla razvoja programske opreme.
3. Pregled omrežne varnosti. Pregled notranjih in zunanjih povezav do sistema, varnost perimetra, pregled požarnih zidov, seznamov za dostop na usmerjevalnikih, pregled odprtih vrat ter postopkov zaznavanja vdorov so tipični primeri.
4. Pregled zagotavljanja neprekinjenega poslovanja. Je področje pregleda obstoja in vzdrževanja na odpoved odporne in redundantne strojne opreme, postopkov izdelave rezervnih kopij in njihovega shranjevanja ter dokumentiranega in preverjenega načrta neprekinjenega poslovanja.
5. Pregled integritete podatkov. Namen tega skrbnega preiskovanja je preverjanje zadostnosti kontrol in vpliv ugotovljenih pomanjkljivosti. Testiranje je možno opraviti tudi s programsko opremo za splošno revidiranje.

Da bi lahko vodstvu predstavili jasno oceno sistema, morajo biti preverjeni vsi ti elementi. Uporabniška programska oprema je namreč lahko implementirana z vsemi varnostnimi možnostmi, a privzeto geslo administratorja sistema ni bilo spremenjeno v operacijskem sistemu strežnika. Takšen primer izniči vse varnostne napore, ki so bili vloženi v izdelavo varne uporabniške programske opreme.

Pri tem je nujno razumeti, da bo vsaka revizija upoštevala te elemente v različnem razmerju oz. z različnim poudarkom. Nekatere revizije bodo morda celo izpustile podroben pregled posameznega elementa informacijskega sistema. Kateri elementi so pomembnejši, določi revizor ob spoznavanju okolja revidirane organizacije, ko pripravlja načrt revizije. V načrtu poudari tiste elemente, katerih nedelovanje bi predstavljajo za podjetje največje tveganje. Temu pravimo tudi pristop, ki temelji na tveganju.

REVIZIJA NA PODLAGI TVEGANJA

Revizor se pri reviziji sooča z vprašanji, kaj, kdaj in kako pogosto naj revidira. Zato uporabi pristop, ki temelji na tveganju, s katerim identificira najpomembnejše dele informacijskega sistema, ki jim posveti še posebno pozornost.

Sestavljanje načrta revizije na podlagi tveganja je sestavljeno iz naslednjih postopkov:

1. Izdelava popisa delov informacijskega sistema podjetja ter uvrščanje teh delov v skupine.

2. Ugotavljanje, kateri deli sistema vplivajo na pomembne funkcije ali vire, kot npr. denar, zaloge, stranke, odločanje, in kako neposreden vpliv imajo na te funkcije in vire.
3. Ocena, katera tveganja vplivajo na te sisteme in učinek na poslovne procese.
4. Razvrščanje delov informacijskega sistema glede na ugotovitve v prejšnjih točkah ter določanje prioritet revidiranja, virov, razporeda ter pogostosti revidiranja.

Priprava pred začetkom revidiranja vključuje tudi zbiranje osnovnih informacij o revidirani enoti ter ocenjevanje virov in znanja, potrebnega za revizijo. To zagotavlja, da bodo v postopku revizije uporabljeni primerni viri na najbolj učinkovit način.

V skladu z dobro prakso se revizor pred začetkom revizije sestane z vodstvom in naročnikom revizije ter ponovno predstavi obseg revizije in njen namen. S tem zagotovi dobro razumevanje postopkov na strani naročnika in vodstva ter običajno izboljša učinek priporočil, ki jih predloži na koncu revizije. Hkrati je to priložnost, da revidirana enota predstavi svoj pogled na revizijo.

VARSTVO OSEBNIH PODATKOV IN REVIZIJA

V Sloveniji področje varstva osebnih podatkov podrobneje ureja Zakon o varstvu osebnih podatkov (ZVOP-1).[2] Med drugim je naloga revizorja tudi, da preveri, ali je delovanje informacijskega sistema skladno z zakonodajo (MSR[3]-250). Preverjanje, ali ima informacijski sistem značilnosti, ki jih določa zakon, je torej sestavni del revizije. Zato je revizor neposredno vključen v postopke nadzora upravljanja z osebnimi podatki.

Področje varovanja osebnih podatkov bo revizor zajel širše, kot to določa zakon, saj revizor pridobiva celostno sliko nad stanjem kontrol v informacijskem sistemu. Del teh kontrol predstavljajo tudi kontrole pri varovanju in obdelavi podatkov, ki pa se ne nanašajo le na osebne podatke, temveč na vse, za katere je revizor v postopku ocenitve tveganja ugotovil, da jim mora posvetiti posebno pozornost.

Prav zato lahko pričakujemo, da bo informacijski sistem bolj celovito naslavljal problematiko shranjevanja, varovanja in obdelave podatkov, če bomo problem obravnavali celovito, iz vidika revizije informacijskega sistema in ne le iz vidika inšpekcijskega nadzora po ZVOP-1.

IZPOSTAVLJENOST PODATKOV

Podatki, ki jih shranjujemo v naših informacijskih sistemih, niso postali bolj izpostavljeni le s pretvorbo v elektronsko obliko. Izpostavljenost se je povečala zaradi napredka tehnologij, ki omogočajo, da do podatkov dostopamo po načelu »od koderkoli, kadarkoli«. Posledica tega je, da so naši strežniki priključeni v prostrana omrežja in dostopa do naše uporabniške programske opreme nimajo več samo naši

[2] *Ur.l. RS, št. 86/2004, 113/2005-ZinfP.*

[3] *Mednarodni standardi revidiranja. V slovenski jezik jih prevajajo pri Slovenskem inštitutu za revizijo (http://www.si-revizija.si/revizorji/msr.php).*

uporabniki, temveč vsi, ki so priključeni v prostrano omrežje (večinoma internet). S tem smo na svoje strežnike nehote povabili tudi strokovnjake, ki velikokrat vedo o uporabniški programski opremi in operacijskih sistemih, na katerih se le-ta izvaja, več kot tisti, ki so programsko opremo izdelali. Prevečkrat to pomeni, da znajo zaobiti varnostne mehanizme, ki so jih snovalci in razvijalci programske opreme vanjo vgradili, in lahko zato dostopajo do podatkov brez ustreznega pooblastila, v najslabšem primeru pa jih lahko celo spreminjajo.

Kontrole, namenjene varovanju podatkov, so zato z leti postale ene pomembnejših kontrol v informacijskem sistemu. Na to pa se niso odzvali le lastniki informacijskih sistemov, temveč žal tudi kriminalci, ki prenašajo nekatere svoje dejavnosti tudi na področje informacijskih sistemov. To se nanaša predvsem na nepooblaščeni dostop do podatkov. Javnost je največkrat obveščena o vdorih v informacijske sisteme in nepooblaščenem dostopu do osebnih podatkov, katerih posledica je zloraba kreditnih kartic, vdori, ki so lahko tudi večjih razsežnosti in imajo vpliv le na posamezna podjetja oz. organizacije, pa velikokrat ostanejo prikriti. V zadnjem času se predvsem v tujini pojavlja tudi t. i. kraja identitete – zavestno zbiranje podatkov o posamezniku z namenom, da si napadalec s pomočjo teh podatkov pridobi finančno korist.

Tega se zaveda tudi Evropska unija, ki skuša problematiko zajeziti z direktivo 95/46/EC, ki opisuje številne zahteve za legitimno upravljanje zbranih osebnih podatkov[2]. V okviru nacionalne zakonodaje jo udejanja ZVOP-1.

Revizorja torej zavezujejo k skrbnemu pregledu upravljanja z osebnimi podatki ne samo zakon, temveč tudi direktiva EU in nenazadnje smernice revidiranja.

Izkušen revizor se bo zavedal, da formalne listine, ki le zadostijo zahtevam ZVOP-1, ne služijo svojemu namenu in da to tudi ni bil cilj zakona in direktive. Zato bo preveril, ali podjetje oz. njegovi zaposleni dejansko izvajajo definirane postopke in kontrole za varstvo osebnih podatkov. Nenazadnje je lahko prekršek zaradi nedoslednega spoštovanja zakona še najmanjša škoda, ki jo utrpi podjetje v primeru, da so osebni podatki kompromitirani. Posledice se lahko raztezajo do dejanske finančne izgube zaradi kraje identitete ali celo do izgube pomembnih strank zaradi diskreditacije.

Najšibkejši člen pri varovanju osebnih podatkov je še vedno neinformiran uporabnik, ki se naivno odzove na napad s pomočjo elektronske pošte ali druge oblike socialnega inženiringa. Zato je del celovitega varovanja osebnih podatkov tudi primerno zastavljeno izobraževanje in informiranje zaposlenih.

Sodelovanje z revizorjem pri vzpostavljanju primernega okolja za varovanje osebnih podatkov ima še eno prednost. Revizorja že standardi zavezujejo k ekonomičnim in učinkovitim izboljšavam, ki izboljšajo varnost informacijskega sistema. Zato je revizor primeren svetovalec in sogovornik, ki s svojimi priporočili revidirano enoto usmerja k najbolj racionalnim oblikam kontrol, katere bodo najbolj učinkovito in uspešno opravile zaupano jim nalogo.

SKLEP

Čeprav revizor ne more neposredno sodelovati pri pripravi internih pravilnikov in kontrol za zagotavljanje varnosti osebnih podatkov, saj je v tem primeru možno, da bo ob naslednji reviziji kompromitirana njegova neodvisnost, že po svoji funkciji preverja tudi področje varstva osebnih podatkov. K temu ga zavezujejo različni

standardi, ki jih uporablja pri svojem delu, direktive EU in Zakon o varstvu osebnih podatkov.

Lastnosti revizije veljajo v vseh primerih in ne glede na to, kdo je revidirana enota – naj bo to gospodarska družba, zavod, upravna enota ali arhiv.

LITERATURA IN VIRI

- *S. Anantha Sayana, The IS Audit Process, Information Systems Control Journal, Volume 1, 2002.*
- *Steve Kenny, Assuring Data Privacy Compliance, Information Systems Control Journal, Volume 4, 2004.*
- *Tommie W. Singleton, What Every IT Auditor Should Know About Identity Theft, Information Systems Control Journal, Volume 6, 2006.*

SUMMARY

INFORMATION SYSTEM AUDITING IN THE CASE OF PERSONAL DATA PROTECTION

The article discusses information system auditing and its advising role for the management and governance of the information system and identifies some problems concerning collection and protection of personal data. Because of the definition of personal data it is common that some databases of personal data remain unidentified regardless of the efforts of personnel responsible for the assembly of the catalogue of databases of personal data. Data of that nature can also be (inadvertently) archive material. Therefore information system auditing presents one of the approaches to reduce risks for unlawful operation of the organization or its information system.