



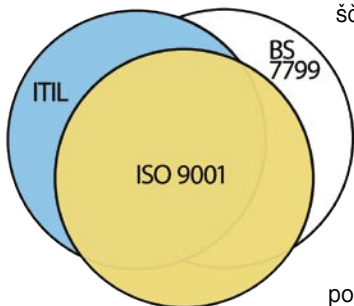
Informacija je dragocena. Ali jo varujete?

..V današnjem tekmovalnem poslovnem okolju so informacije stalno podvržene grožnjam iz mnogo različnih virov, z uporabo sodobnih tehnologij pa se ogroženost samo povečuje. Ste se že kdaj vprašali, kje vse se nahajajo informacije vašega podjetja, kdo vse ima do njih dostop in predvsem, kdo vse lahko ogrozi te informacije ali pa jih zlorabi?..

Informacije predstavljajo nujno potrebno "življenjsko tekočino" podjetij in lahko obstajajo v mnogoterih oblikah - napisane ali tiskane na papir, shranjene na različnih medijih, posredovane elektronsko ali preko običajne pošte, podatkovne zbirke, govorne informacije itd. Zavedati se moramo, da so informacije ravno tako delovno sredstvo, kot so delovno sredstvo tudi oprema, stroji in naprave v posameznem podjetju. Ker so informacije sredstvo, jih je potrebno ustrezno zaščititi, jih ustrezno varovati, oziroma na kratko rečeno, z informacijami je potrebno upravljati.

Dandanes je postalo nekako samoumevno, da imajo vsi računalniki nameščen protivirusni program, da se redno izdelujejo varnostne kopije podatkov v računalnikih, itd. S tem je prišlo tudi do povsem zgrešenega mišljenja, da je varovanje informacij in upravljanje z njimi predvsem domena informatikov. Predstavljajmo si preprost primer: popolnoma varovan informacijski sistem, uporabnik izpiše podatke preko tiskalnika na papir, papir pregleda in ga vrže v koš za smeti. Nekdo na smetišču najde te papirje in zlorabi informacije na njem. Do napake pri varovanju informacij ni prišlo zaradi napake informatikov, pač pa zaradi nepravilnega ravnanja zaposlenega in njegove nizke za-vesti o pomembnosti varovanja informacij.

Zavedati se moramo, da najnoveše tehnologije in najnoveše tehnične rešitve nikakor ne pomenijo, da bomo v resnici naše informacije ustrezno zaščitili in jih varovali.



Pri varovanju informacij je najpomembnejši dejavnik človek. Zato je potrebno določiti odgovornost posameznika za

posamezno informacijo ter dvigniti zavest o pomembnosti informacij in njihovi veliki poslovni vrednosti.

Odtokanje informacij in njihove zlorabe se najpogosteje dogajajo izven IT oddelkov. Temu se lahko uspešno izognemo brez velikih investicij, predvsem z organizacijskimi spremembami znotraj podjetja. Kot primer lahko služi zahteva, da zaposleni ne smejo imeti na svoji delovnih mizah razmetanih dokumentov, na katere lahko "vrže oko" vaša morebitna stranka ali konkurenca.

Ker se z zlorabami informacij srečujejo po celem svetu, je bil za ustrezno upravljanje varovanja informacij razvit standard, ki temelji na izkušnjah, dobrih praksah in predvsem "zdravi pameti".

Standard upravljanja varovanja informacij je objavljen v dveh delih: ISO/IEC 17799 Code of practice for Information Security Management ter BS 7799-2:2002 Specification for Information Security Management, ki sta v Sloveniji sprejeta v izvorni različici.

Znotraj regulative EU najdemo regulative o elektronskih komunikacijah, elektronskem podpisu, zaščiti zasebnosti, računalniškem kriminalu, informacijski varnosti itd., ki vsebujejo elemente standarda BS 7799. Implementacija standarda BS 7799 je nujno zlo tudi za vse tiste, ki želijo pridobiti sredstva PHARE, ISPA, SAPARD itd. V Sloveniji je nekaj pravnih podlag, ki bodisi eksplicitno narekujejo uporabo standarda BS 7799 bodisi nam to narekuje zdrava pamet, če želimo maksimalno zadostiti zahtevam: Zakon o varstvu osebnih podatkov (ZVOP-1), Zakon o bančništvu, Priporočila za pripravo informacijske varnostne politike CVI, Zakon o investicijskih skladih in družbah za upravljanje (ZISDU-1) itd.

V podjetju lahko standard uvaja nekdo, ki ima znanja, potrebne izkušnje in kvalifikacije za takšno početje in je deležen popolne podpore najvišjega vodstva v podjetju. V nasprotnem primeru je projekt uvajanja standarda že v osnovi obsojen na propad. Podjetje lahko uvaja standard s pomočjo zunanje svetovalne hiše, ki ima usposobljene strokovnjake za tovrstno dejavnost. Nekatere svetovalne hiše imajo partnerske pogodbe s certifikacijskimi telesi. Podjetje, ki ima sklenjeno takšno pogodbo, že s tem dokazuje resnost delovanja na tem področju. Toda uvajanje standarda na ta način ne pomeni, da bo celotno delo opravila zunanja svetovalna hiša. Sistem mora zelo dobro živeti v harmoniji z organizacijsko kulturo v podjetju, v harmoniji z ljudmi, ki so v podjetju zaposleni. Sistem so ljudje in če ljudi ne prepričate v to, da je varovanje informacij potrebno in da so del tega tudi zaposleni v podjetju, sistem ne bo deloval. Uvajanje sistema je seveda lahko tudi kombinacija obeh omenjenih načinov uvajanja. (P.R.)



Danesa, informatika, svetovanje in posredništvo d.o.o.
 Legatova 2, p.p. 4555
 1001 Ljubljana
 tel: +386 1 242 9000
 faks: +386 1 242 9010
 www.danesa.com
 e-mail: info@danesa.com