K. Klasić*

ZAŠTITA INFORMACIJSKIH SUSTAVA U POSLOVNOJ PRAKSI

UDK 004.056.5
PRIMLJENO: 8.3.2006.
PRIHVAĆENO: 4.1.2007.

SAŽETAK: Primjena informacijskih tehnologija u svakodnevnom radu u stalnom je porastu. Dok je još prije samo desetak godina relativno mali broj zaposlenika za obavljanje svojih radnih obveza koristio računalo, danas je nezamislivo zaposliti novog djelatnika koji ne poznaje rad na računalu. Broj sati aktivnog rada za računalom raste, pri čemu se to ne odnosi samo na tvrtke koje se bave informatičkom djelatnošću. Stoga se stručnjaci za zaštitu na radu sve češće susreću s različitim problemima iz domene primjene računala u poslovnoj praksi, a koji direktno ili indirektno utječu na rezultate rada.

Svako poduzeće posjeduje vlastiti informacijski sustav koji može, ali i ne mora biti podržan računalom. Ipak, danas je informacijska tehnologija duboko prodrla u sve pore poslovanja i svakodnevnog života, na što je značajno utjecala decentralizacija opreme i programske podrške (softvera). Pri tomu se često nije predviđala adekvatna zaštita računala i podataka, a postojeća pravila koja su se primjenjivala u centraliziranim računalnim centrima nisu se ažurirala. Uvođenje internetske tehnologije samo je pridonijelo nesigurnosti informacijskih sustava. Korisnici informacijskog sustava ili nekog njegova segmenta ponekad nisu ni upoznati s potrebom i značenjem podatkovnih resursa poduzeća kao ni načinima njihove zaštite. Podaci su osnovni resurs poslovnog sustava tako da se šteta nastala njihovom zloporabom (ili gubitkom, pogrešnom uporabom i slično) zapravo nanosi poduzeću u cjelini. Stoga je organizacija zaštite informacijskog sustava interdisciplinarni zadatak svih zaposlenika poduzeća kojem je cilj ostvariti što viši stupanj sigurnosti u skladu s prihvatljivim gubicima s kojima poduzeće mora računati. U tu svrhu najčešće se primjenjuju različiti dokumenti koji se odnose na pojedine aspekte zaštite sustava, a koji se uglavnom kreiraju i počinju primjenjivati tek kada se dogodi neki od oblika narušavanja sigurnosti sustava. U praksi se obveza izrade i primjene takvih dokumenata uglavnom propisuje posebnim pravilnikom, a tek rijetka poduzeća počinju uvoditi model zaštite informacijskog sustava u skladu s međunarodnom normom ISO/IEC 17799:2000.

Također, zaštita radnika koji svakodnevno obavljaju svoj posao uz primjenu računala mora se provoditi u skladu s Pravilnikom o sigurnosti i zaštiti zdravlja pri radu s računalom. Njime su propisani zahtjevi koje računalna oprema mora zadovoljavati, te je propisana obvezna izrada procjene opasnosti za ta radna mjesta.

Zaštita informacijskog sustava zajednička je odgovornost svih zaposlenika tvrtke, tako da samo zdravi, zadovoljni i adekvatno educirani radnici, koji rade u primjerenim uvjetima rada, mogu pridonijeti unapređenju sigurnosti opreme i podataka u poslovnom sustavu.

Ključne riječi: i*nformacijski sustav, zaštita informacijskog sustava, zaštita na radu, ergonomija, ISO/IEC 17799:2000, Pravilnik o sigurnosti i zaštiti zdravlja pri radu s računalom*

* Doc. dr. sc. Ksenija Klasić, K & K posredovanje u osiguranju d.o.o., III. bijenički odvojak 18, 10000 Zagreb.

UVOD

Sigurnost podataka i zaštita informacijskih sustava dugo godina su smatrani ekskluzivnim pravom, ali i obvezom informatičkih stručnjaka. S obzirom na to da se radilo o djelatnosti koja je zahtijevala specifična znanja u području informacijskih tehnologija, a koja su često bila nedostupna većem broju zaposlenika, nije se ni posvećivala adekvatna pozornost ovoj problematici. Tek s porastom primjene računala u poslovnoj praksi počeli su se uvoditi prvi standardi koji su se odnosili na siguran rad s računalima i podacima pohranjenim u informacijskim sustavima. U početku je bio presudan značaj fizičke zaštite sustava jer je računalna oprema bila centralizirana, uglavnom u dobro čuvanim posebnim objektima ili prostorima. Distribucijom opreme i podataka te uključivanjem u internet, potreba za zaštitom sustava postala je još važnijom, ali i znatno složenijom. Prepoznavanje te potrebe ogleda se u izradi i primjeni raznih uputa o zaštiti podataka koji se primjenjuju u poduzećima. Unatoč tomu još uvijek postoji velik broj organizacija koje ne razumiju potencijalne opasnosti kojima su izloženi njihovi informacijski sustavi i stoga ih nedovoljno štite. Pri tome je zapostavljena i uloga zaposlenika koji svojim djelovanjem mogu hotimice[1], ali i nehotično nanijeti nemale štete poduzeću u kojem rade. Do zloporabe uglavnom dolazi iz dvaju razloga:

- zbog ostvarivanja neopravdanih ili protupravnih koristi od pojedinaca ili organiziranih skupina, ili
- zbog nanošenja materijalne ili nematerijalne štete pojedincu, skupini ili zajednici.

Pri tome su najugroženiji informacijski sustavi iz kojih se može pristupiti internetu, jer je i sam internet iznimno ugrožen[2].

U Hrvatskoj se za sada ne prikupljaju (ili barem nisu javno objavljeni) konkretni podaci o problemima sa sigurnošću sustava, no zacijelo nemali broj poduzeća i institucija ima svakodnevne probleme koji se za sada ili promptno rješavaju ili se zataškaju zbog mogućeg negativnog utjecaja na poslovanje.

Stoga je u 2003. godine provedeno istraživanje[3] na uzorku od 37 hrvatskih poduzeća i njime je utvrđeno da:

- u 27% tvrtki je u posljednje dvije godine došlo do šteta na informatičkoj opremi i podacima od požara, strujnog udara, zbog nestručnog rukovanja, kvara na disku, pada sustava, izgubljenih datoteka, «pregaženih» dokumenata i slično,
- 49% navodi da je u 2002. godini neko od računala bilo zaraženo virusom,
- u 16% tvrtki bilo je pokušaja neovlaštenog pristupa podacima i računalima,
- 35% tvrtki kontrolira pristup internetu, 32% zbog sigurnosne kopije podataka, a samo u 30% štiti se fizički pristup računalima, dok se informacijski sustav uglavnom štiti putem korisničkih lozinki (78%) i antivirusnim programima (57%),
- 43% tvrtki navodi da ne postoji rezervni plan za slučaj prekida rada informacijskog sustava, niti su od te opasnosti osigurane kod nekog osiguravajućeg društva.

Treba istaknuti da se u čak 43% poduzeća upotrebljavaju dokumenti koji se odnose na pojedine aspekte zaštite informacijskog sustava, ali da nema interdisciplinarnog pristupa organizaciji sigurnosti.

Iz navedenog istraživanja moglo se zaključiti da su korisnici informatičke tehnologije prepoznali potrebu zaštite informacijskih sustava, te su u skladu sa svojim mogućnostima i znanjima pokušavali organizirati vlastite sustave zaštite. Može se uočiti da se zaštita uglavnom odnosila na fizički pristup računalima[4] te na kontrolu pristupa podacima koji su pohranjeni na računalima.

[1] Prema nekim istraživanjima čak do 80% ukupnih napada na sustav odnosi se na zloporabe od zaposlenika tvrtke!

[2] U EU se preporuča kažnjavanje hakera i širitelja virusa zatvorskim kaznama. Prekršiteljima zakona smatraju se svi oni koji ilegalno pokušavaju ući u računalne mreže i poslužitelje, te oni koji namjerno šire računalne viruse. Ranjivost interneta navela je SAD da poveća nacionalnu cyber sigurnost – tamo se predlaže da hakeri koji preko interneta ugroze živote drugih ljudi mogu biti osuđeni na doživotni zatvor, a tretirat će ih se kao opasne teroriste.

[3] K. Klasić: Organizacija zaštite informacijskih sustava, Suvremeno poduzetništvo, br. 5, str. 80-88, 2003.

[4] Većina anketiranih tvrtki imala je iskustva s organizacijom fizičke i tehničke zaštite svojeg poslovnog prostora.

Smanjenje veličine računala i ostalog očvrsja (hardvera) utjecalo je na razinu fizičke zaštite. Dok su postojali isključivo veliki računski centri, zaštiti se pridavala odgovarajuća pozornost. U računskom centru koncentrirana je računalna oprema (posebice u velikim sustavima kao što su vojska, policija, državna uprava, banke, osiguravajuća društva), pa ga je često lakše zaštititi. Fizička zaštita računala koja se nalaze u uredima, ponekad i u neadekvatnim prostorima uglavnom je zapostavljena. Oprema koja se nalazi na radnim stolovima zaposlenika štiti se u sklopu ostalih sigurnosnih aktivnosti koje bi trebalo provoditi u poduzeću. Nemar prema sigurnosti podataka pohranjenih na prijenosnim računalima posebno je izražen (ne samo u nas, o čemu gotovo svakodnevno svjedoči dnevni tisak).

U ožujku 2005. godine Vlada Republike Hrvatske donijela je Nacionalni program informacijske sigurnosti[5], kojim se definiraju ciljevi informacijske sigurnosti na razini države, nadležnosti i poslovi pojedinih institucija u području informacijske sigurnosti kao i potrebnu međusobnu koordinaciju svih čimbenika informacijske sigurnosti. Strateška zadaća ovog Nacionalnog programa je postupno širenje procesa informacijske sigurnosti na državu u cjelini, uvođenjem odgovarajućih minimalnih sigurnosnih kriterija u državni i javni sektor te razvojem sigurnosne kulture najširih slojeva stanovništva.

Za potrebe ovog razmatranja posebno treba izdvojiti poglavlje koje se odnosi na edukaciju i razvoj sigurnosne kulture, a u kojem se navodi «da u RH ne postoje specijalizirane škole ili smjerovi za obuku stručnjaka za informacijsku sigurnost. Nema niti sustavne organizacije tečajeva ili drugih oblika cjeloživotnog obrazovanja[6]». Iz navedenog citata razvidno je da u tvrtkama postoji potreba za dodatnom edukacijom zaposlenika. No, najčešće se ne radi samo o informatičkoj edukaciji, već i o svim ostalim elementima koji čine rad na siguran način na radnom mjestu s računalom.

MODELI ZAŠTITE INFORMACIJSKIH SUSTAVA U POSLOVNOJ PRAKSI

Planiranje zaštite informacijskog sustava trebalo bi biti dio aktivnosti primjene računala u poslovnom sustavu. Stoga je ISO organizacija[7] u sklopu zajedničkog tehničkog komiteta IEC JTC 1 (*engl. Joint Technical Commity*) organizirala potkomitet broj 27 putem kojeg nastaju norme za sigurnost informacijskog sustava[8].

Prve norme koje se odnose na uspostavu cjelovitih sustava upravljanja sigurnošću u informatici objavio je British Standard Institute (BSI) 1995. godine kao dvije norme pod zajedničkim nazivom BS 7799:1995. Te su norme preuzete i neznatno modificirane, te objavljene kao norma ISO/IEC 17799:2000.

Svrha norme ISO/IEC 17799 je uspostava organizacijske kontrole i upravljanja zaštitom informacijskog sustava (odnosno njegovom sigurnošću) u poslovnom sustavu[9]. S obzirom na specifičnosti svakog pojedinog sustava, ova norma daje preporuke i nužne elemente koje bi trebalo poštovati pri izradi i primjeni vlastitog modela upravljanja sigurnošću i čini prvi dio norme BS 7799. Drugi dio norme BS 7799 specificira zahtjeve za uspostavljanje, primjenu, održavanje i poboljšanje sustava upravljanja sigurnošću informacija i za taj dio norme se certificira.

U Hrvatskoj je samo jedna tvrtka uspjela proći zahtjevan postupak usklađivanja sigurnosnih pravila informacijskog sustava s BS 7799-2 standardom te je dobila sveobuhvatni i najšire priznat certifikat za informacijsku sigurnost u svijetu[10]. To je CS Computers Systems kojoj je certifikat dodijelila tvrtka Det Norske Veritas.

[5] www.e-hrvatska.hr

[6] Nacionalni program informacijske sigurnosti, str. 71.

[7] **ISO** - *The International Organization for Standardization* - svjetsko udruženje nacionalnih institucija za normizaciju. ISO članice predlažu norme i svaka nova norma prihvaća se kada ju prihvati najmanje 75% svih ISO članica.

[8] Do 2000. godine nastale su takve 33 norme koje su uglavnom tehničke norme i obuhvaćaju samo jedan aspekt sigurnosti poput, primjerice, ISO/IEC 9786-2: 1997. Information technology- Security techniques-Digital signature shemes giving message revcovery- Part 2. Mechanism using a hast function ili ISO/IEC 9798-4:1999 Information technology- Security techniques-Entity authentification -Part 4: Mechanisms using a criptographic check function.

[9] Prema Zebec Koren, M. i Ključevšek, R.: Sustav upravljanja informatičkom sigurnošću, Svijet osiguranja, br. 5/2001, Tectus, Zagreb.

[10] www.vlast.net, 23.05.2005.

Ova norma razlikuje tri temeljna oblika upravljanja sigurnošću informacija:

a. pouzdanost, odnosno pristup nužnim informacijama koji se dopušta samo ovlaštenim korisnicima,
b. cjelovitost, što uključuje zaštitu od izmjena ili oštećenja, te brigu o točnosti i cjelovitosti podataka,
c. dostupnost, što znači da se informacije stavljaju na raspolaganje prema potrebi i u sklopu određenog konteksta.

Ključan element pri provedbi zaštite sustava je podrška poslovodstva. Poslovodstvo donosi smjernice politike sigurnosti te daje podršku za njezinu primjenu. Uz ovu normu nužno je primjenjivati i ostale norme koje se odnose na tehnike sigurnosti informatičke tehnologije, a koje propisuju i nadziru informatički stručnjaci.

Međutim, budući da je zaštita informacijskog sustava posao koji zahtijeva rad tima stručnjaka različitih profila, uloga poslovodstva je i u organiziranju operativne provedbe zaštite kao i u animiranju svih zaposlenih za provođenje politike sigurnosti u tvrtki. Stoga struktura norme ISO 1799:2000 (a koja je u skladu s BS 7799) može poslužiti za razlikovanje deset mogućih procesa u tvrtki koji su povezani s upravljanjem kontrole sigurnosti. Struktura norme ISO/IEC 17799:2000 prikazana[11] je u Tablici 1.

Detalje o normi moguće je naći na mrežnim stranicama[12] poput, primjerice www.iso17799software.com, www.iso17799.net, www.dnv.hr itd. Na njima se opisuje što je zapravo ta norma, odnosno koja je njezina namjena, prezentira se njezina struktura u deset poglavlja te daju smjernice kako ju primijeniti.

Tablica 1. Struktura norme ISO/IEC 17799:2000
Table 1. Standard ISO/IEC 17799:2000

Uvodni dio	
• Namjena norme	
• Terminologija	
Sadržaj norme	
1.	Politika sigurnosti koja se izrađuje u obliku posebnog dokumenta
2.	Organizacijska sigurnost koja uključuje način organizacije provedbe politike sigurnosti u poduzeću
3.	Klasifikacija i nadzor imovine koja se primarno odnosi na imovinu informacijskog sustava
4.	Sigurnost osoblja koja uključuje upravljanje ljudskim resursima i zaštitu tajnosti podataka
5.	Fizička sigurnost i sigurnost okoline kojom se štiti fizički pristup imovini informacijskog sustava
6.	Upravljanje komunikacijama i operativom koje uključuje zaštitu logičke imovine od svih vrsta zloporaba
7.	Kontrola pristupa kojom se štiti pristup resursima informacijskog sustava od neovlaštenih korisnika iz poduzeća, ali i putem mreže
8.	Razvoj i održavanje sustava kojim se propisuje način ugradnje zaštite resursa sustava u tijeku razvoja i primjene informacijskog sustava
9.	Upravljanje kontinuitetom poslovnih aktivnosti kojim se sprečavaju prekidi poslovnih aktivnosti i štite kritični poslovni procesi, te
10.	Usklađenost sa zakonskom regulativom, te ocjena politike sigurnosti i suglasnosti s tehničkim uvjetima

[11] Krakar, Z.: Sustavi sigurnosti u informatici kao dio kvalitete sustava, Savjetovanje CASE 13, Opatija 2001.

[12] Unosom ključne riječi "17799" pretraživači nude pristup do mrežnih stranica koje se odnose na ISO normu, dok ključna riječ "7799" vodi do norme BS 7799 za koju se mogu pronaći i informacije o tvrtkama koje imaju odgovarajući certifikat.

Model organizacije zaštite informacijskog sustava koji se temelji na primjeni norme ISO/IEC 17799:2000 sukladan je sadržaju norme. To znači da je prvi korak promišljanje poslovodstva o politici sigurnosti u tvrtki, te izrada i prihvaćanje pisanog dokumenta koji služi kao kostur cijelog modela organizacije sigurnosti. Njime se određuje redoslijed i okvirni sadržaj poslova koji treba napraviti pri realizaciji zacrtane politike sigurnosti. Stoga je sljedeći korak izrada dokumenta kojom se propisuje organizacijska sigurnost. Njome se određuje način organizacije upravljanja informatičkim resursima i provedbe politike sigurnosti u poduzeću, način upravljanja sigurnošću kada informatičkim resursima mogu pristupati treće osobe, kao i u slučaju kada je odgovornost za procesiranje podataka iz usluge predana drugoj tvrtki, odnosno vanjskom poslovnom partneru (*engl. outsourcing*[13]).

Klasifikacija i nadzor imovine informacijskog sustava sastoji se od dvije faze:

- izrađuje se popis cjelokupne imovine informacijskog sustava, te se popisana imovina klasificira,
- određuje se razina sigurnosti za popisanu opremu, te osobe odgovorne za njezinu provedbu.

Kategorije imovine informacijskog sustava za koju treba odrediti razine sigurnosti prikazane su u Tablici 2.

Cilj dokumenta koji se odnosi na sigurnost osoblja je smanjenje rizika nehotičnih ljudskih pogrešaka, krađe, prijevare kao i zloporabe. Potencijalne zaposlenike koji bi trebali raditi na informatičkim poslovima treba psihološki obraditi i provjeriti njihova načela i stavove prije zapošljavanja, a u ugovor o radu mora biti uključena odredba o čuvanju poslovne tajne, te sankcije za slučaj prekršaja. Korisnici informacijskog sustava moraju biti upoznati s mogućim opasnostima i adekvatno educirani za provođenje svakodnevnih sigurnosnih mjera. U tu svrhu izrađuje se plan i program osposobljavanja korisnika, po pojedinim radnim mjestima. Ipak, ponekad se događa da zaposlenici onesposobljavaju fizičku imovinu informacijskog sustava ili sredstva telekomunikacije (sabotaža), zatim da informacijski sustav koriste za vlastite potrebe ("krađa vremena" ili "krađa usluga"), kao i da nehotice, slučajno, aktiviraju neki od programa za koji ni ne znaju da može biti zloupotrijebljen.

Također, potrebno je utvrditi ergonomske kriterije koje moraju zadovoljavati radna mjesta s računalima.

Tablica 2. Kategorije imovine informacijskog sustava

Table 2. Information system ownership categories

Kategorija	Tip imovine	Primjeri
Očvrsje	Fizička	Računala, periferne jedinice, komunikacijska oprema i veze
Oprema	Fizička	Namještaj, energetska oprema, uredska oprema, skladišna oprema
Dokumentacija	Fizička	Sustavna i programska dokumentacija, dokumentacija baze podataka, standardi, planovi, police osiguranja, ugovori
Zalihe materijala	Fizička	Papir, diskete, CD, DVD, trake, ostali potrošni materijal
Podaci/informacije	Logička	Aktivne, pričuvne i arhivske datoteke
Aplikacijska program. podrška	Logička	Sve vrste aplikacijskih programa i alata
Sustavna program. podrška	Logička	Operacijski sustavi, sustavi za upravljanje bazom podataka, programi prevoditelji, pomoćni programi

**Izvor: Panian, Ž.: Kontrola i revizija informacijskih sustava, Sinergija, 2001., str. 59.*

[13] Nacionalni program informacijske sigurnosti u RH primjer je takvog dokumenta.

Fizička sigurnost i sigurnost okoline odnosi se na sprečavanje neovlaštenog pristupa resursima informacijskog sustava, šteta te krađe podataka ili medija za pohranu i prijenos podataka tvrtke. Zaštitne mjere koje treba pri tome primjenjivati propisuju stručnjaci za područje zaštite na radu i tehničke zaštite.

Upravljanje komunikacijama i operativom (što se uglavnom odnosi na upravljanje računalnim mrežama) mora osigurati sigurnost podataka koji kolaju mrežom kao i zaštititi informatičku infrastrukturu koja podržava komunikaciju. Cilj dokumenta je smanjiti rizik nemogućnosti rada računala, odnosno osigurati neprekidnu dostupnost podacima i programima svima kojima je to potrebno, osigurati zaštitu integriteta programske podrške i podataka, čime se sprečava prekid poslovnih aktivnosti tvrtke, kao i spriječiti gubitke, neovlaštene izmjene ili zloporabu podataka koji se razmjenjuju među raznim organizacijama.

Idući korak je kontrola pristupa, čiji je cilj upravljati pristupanjem podacima i mreži. Moraju biti propisane procedure za sprečavanje neautoriziranog pristupa podacima u sustavu, ali i računalu u mreži. Time se omogućava otkrivanje svih neautoriziranih aktivnosti jer je iskustvo pokazalo da ih ponekad nije moguće u potpunosti spriječiti. Pravovremenim utvrđivanjem pojave neovlaštenog pristupa zlonamjernog korisnika ili hakera, moguće je smanjiti štetu koji oni mogu prouzročiti. Procedure kojima se određuje postupanje u slučaju potrebe za rekonstrukcijom podataka ili obnovom dijela informacijskog sustava moraju biti definirane u sklopu aktivnosti kontrole pristupa.

Dokument koji se odnosi na razvoj i održavanje sustava mora osigurati da je zaštita ugrađena u informacijski sustav u procesu razvoja sustava, te da su spriječeni gubici, neovlaštene izmjene i zloporabe podataka aplikacijskog sustava. Svaka aplikacija mora imati ugrađene propisane kontrole podataka, odnosno provjeru ispravnosti (validaciju) ulaznih podataka, kontrolu obrade podataka, provjeru autentičnosti poruka i provjeru ispravnosti izlaznih podataka. Postupci i kontrole moraju biti izrađeni u pisanoj formi, a najčešće ih izrađuju informatičari zajedno s korisnicima sustava.

Dokumente kojima se određuju standardi i pravila postupanja kod upravljanja komunikacijama i operativom, kod kontrole pristupa i kod razvoja i održavanja sustava uglavnom izrađuju informatički stručnjaci, koji su nadležni i za kontrolu njihova provođenja.

Upravljanje kontinuitetom poslovnih aktivnosti odnosi se na sprečavanje prekida poslovnih aktivnosti neovisno o uzroku. Stoga se obvezno izrađuje popis svih kritičnih poslovnih procesa, odnosno onih koji su nužni za poslovanje tvrtke, izrađuju se planovi «što–ako», tj. kako postupati ako nije moguće obavljati redovne aktivnosti, te se određuju osobe odgovorne za pojedine segmente posla. Planove je potrebno redovito ažurirati i prilagođivati promjenama i u tehnologiji i u poslovanju. U ovome poslu sudjeluju zaposlenici tvrtke zajedno sa stručnjacima za pojedina poslovna područja, odnosno za zaštitu na radu i tehničku zaštitu.

Zadnji korak je usklađivanje sa zakonskom regulativom, te ocjena politike sigurnosti i suglasnosti s tehničkim uvjetima. Pri tome se identificiraju zakoni koji se mogu primijeniti na zaštitu informacijskih sustava, primjenjuju propisi koji se odnose na zaštitu i tajnost podataka, intelektualno vlasništvo, zaštitu privatnosti. Preporuka je važeću zakonsku regulativu ugraditi u interne dokumente, gdje god je to moguće.

Rezultat ovog modela organizacije zaštite informacijskog sustava je niz dokumenata koji proizlaze iz svakog pojedinog koraka. Tijekom provjere ovlaštene organizacije za certfikaciju moraju biti u stanju procijeniti jesu li istaknute kritične točke doista važne i je li primijenjena razina zaštite odgovarajuća i povezana u odnosu na procjenu rizika/upravljanje rizicima.

U Hrvatskoj ne postoji obveza primjene norme ISO/IEC 17799:2000, odnosno BS 7799. Stoga je u praksi u nekim hrvatskim poduzećima umjesto ove norme primijenjen model pravilnika o zaštiti informacijskog sustava[14].

[14] Često ga zovu pravilnikom o zaštiti podataka, čime je obuhvaćen samo jedan segment zaštite informacijskog sustava.

Njime se navode osnovni elementi zaštite sustava u poduzeću, a detalji se razrađuju u posebnim, dodatnim dokumentima, koji su podložni češćim revizijama, posebno zato što se tehnologija iznimno brzo razvija i mijenja. Iako osnovna struktura pravilnika o zaštiti informacijskog sustava može za svaku tvrtku biti jednaka, svako poduzeće mora i pravilnik i dodatne dokumente prilagoditi vlastitom poslovanju[15].

Primjer strukture pravilnika o zaštiti informacijskog sustava prikazan je u Tablici 3.

Dodatne dokumente, koji su potrebni uz pravilnik o zaštiti informacijskog sustava, svakako treba najmanje jedanput godišnje ažurirati ili u potpunosti zamijeniti. To su primjerice:

- popis instaliranog očvrsja i programske podrške
- uputa za rad s informatičkom opremom

Tablica 3. Moguća struktura pravilnika o zaštiti informacijskog sustava

Table 3. A possible guide for the regulations on information system security

I.	OPĆE ODREDBE
II.	PREDMET ZAŠTITE INFORMACIJSKOG SUSTAVA
III.	IZVORI UGROŽAVANJA INFORMACIJSKOG SUSTAVA • Zloporaba • Izvori ugrožavanja vezani uz informatičare, korisnike informacijskog sustava i ostale osobe • Organizacijski izvori ugrožavanja • Izvori ugrožavanja vezani uz očvrsje i programsku podršku • Elementarne nepogode, požari, neposredna ratna opasnost, rat i druge izvanredne prilike • Ostali izvori ugrožavanja
IV.	MJERE I AKTIVNOSTI ZAŠTITE INFORMACIJSKOG SUSTAVA • Obveze i odgovornosti svih djelatnika • Kadrovske mjere zaštite • Obrazovne mjere zaštite • Mjere zaštite na radu • Organizacijske mjere zaštite • Normativno-pravne mjere zaštite • Fizičke i tehničke mjere zaštite • Mjere zaštite za očvrsje i programsku podršku • Protuelektroničke mjere zaštite • Mjere kriptografske zaštite • Mjere zaštite od požara i poplave • Zaštita poslovne tajne tvrtke u sklopu IS • Postupak u slučajevima zastoja ili kvara na informatičkoj opremi • Zaštita i mogućnost funkcioniranja informacijskog sustava u slučaju elementarnih nepogoda, požara i slično • Zaštita i mogućnost funkcioniranja informacijskog sustava u slučaju neposredne ratne opasnosti, rata i drugih izvanrednih prilika
V.	ODBOR ZA ZAŠTITU INFORMACIJSKOG SUSTAVA
VI.	ZAKLJUČNE ODREDBE

[15] Primjer sadržaja pravilnika nalazi se u Klasić, K: «Zaštita informacijskih sustava», IPROZ, Zagreb, 2002.

- plan zaštite, odnosno uputa o načinu funkcioniranja i zaštiti informacijskog sustava
- uputa za zaštitno kopiranje podataka informacijskog sustava
- uputa o zaštiti od virusa
- uputa o zaštiti pristupa računalima i podacima informacijskog sustava
- način dodjele, čuvanja i mijenjanja lozinki u informacijskom sustavu
- način dodjele ovlaštenja za pristup internetu
- pravilnik o nabavi očvrsja i programske podrške
- mjere fizičko-tehničke zaštite prostora u kojima se nalazi informatička oprema
- uputa o zaštiti podataka i informacija koje se prenose informatičkom mrežom
- preventivne mjere zaštite tajnih podataka
- uputa o prijavi kvara i načinu otklanjanja kvarova na informatičkoj opremi
- plan oporavka informacijskog sustava u slučaju katastrofe, itd.

Iako se navode u pravilniku, dodatni dokumenti se često u tvrtkama izrađuju *ad hoc*, bez utvrđenog tehnološkog pravila, a neki se nikada niti ne oblikuju u pisanoj formi. Standardizacija dokumentacije i uvođenje norme ISO 9000 zahtijeva propisane procedure postupanja s dokumentima, čime se značajno unapređuje i zaštita informacijskog sustava[16].

Informacijski sustav može se zaštititi i sklapanjem odgovarajuće police osiguranja, čime je obuhvaćena uglavnom fizička imovina informacijskog sustava, a tek ponekad i podaci. Međutim, ozbiljni osiguravatelji zahtijevaju od svojih osiguranika planiranje zaštite informacijskog sustava i provođenje sigurnosnih preventivnih mjera. Time se smanjuje mogućnost nastanka štete, te podiže opća razina informacijske kulture zaposlenika.

U početku primjene informacijske tehnologije u poslovanju osiguravajuća društva su računala i ostalu pripadajuću elektroničku opremu osiguravala u sklopu osiguranja od požara i osiguranja od loma stroja. S obzirom na sve veću rasprostranjenost primjene informacijske tehnologije u društvu i sve veću važnost pohranjenih podataka, osiguravatelji su u tu svrhu ponudili posebne vrste osiguranja. No, za većinu njih preduvjet je postojanje kvalitetne i dokumentirane interne zaštite informacijskog sustava.

ULOGA ZAŠTITE NA RADU NA RADNIM MJESTIMA S RAČUNALIMA

Uspješnost poslovnog sustava ovisi i o kvaliteti podataka koji se nalaze u informacijskom sustavu, a njihova kvaliteta pak ovisi i o radnim uvjetima pod kojima se podaci unose i obrađuju.

U Hrvatskoj je donesen Pravilnik o sigurnosti i zaštiti zdravlja pri radu s računalom[17] u skladu sa smjernicama EU-a koji određuje da radno mjesto s računalom obuhvaća računalo (sa zaslonom, tipkovnicu i/ili napravu za unošenje i/ili programsku opremu), dodatnu opremu, vanjske jedinice, telefon, modem, držač za predloške, radni stolac, radni stol ili radnu površinu, okruženje koje ima neposredan utjecaj na radno mjesto te radne zadatke zaposlenika.

Poslodavac je obvezan izraditi procjenu opasnosti za sva radna mjesta s računalom, imajući u vidu moguće opasnosti od narušavanja zdravlja radnika, posebice zbog vidnog, statodinamičkog i psihičkog napora. Kako bi se smanjilo opterećenje pri radu sa zaslonom, poslodavac mora planirati aktivnosti radnika na takav način da se rad sa zaslonom tijekom rada periodički izmjenjuje s drugim aktivnostima. Ako to nije moguće, poslodavac mora tijekom svakog sata rada osigurati najmanje 5 minuta odmora i organizirati vježbe rasterećenja.

[16] Osim navedene, u Hrvatskoj se u sklopu prilagodbi zakonodavstvu EU-a uvode i druge norme koje nalažu primjenu zaštite elektronskih zapisa i podataka.

[17] N.N., br. 69/2005.

Prilogom pravilnika određena su načela koje poslodavac treba uzeti u obzir pri oblikovanju, izboru, naručivanju i mijenjanju programske opreme i oblikovanju radnih zadataka pri radu s računalom. Međutim, programska oprema često ne može istodobno zadovoljiti načela da «mora biti takva da se radni zadatak može izvršiti», da «mora biti jednostavna za uporabu i prilagođena znanju radnika» i da «oblik i brzina davanja informacija mora biti prilagođena radniku». Ponekad, posebno u slučaju primjene računala pri obavljanju složenih radnih zadataka, radnici moraju biti dodatno educirani za rad s programskom opremom i moraju zadovoljavati određene stručne, ali i psihofizičke preduvjete. Nije za očekivati da će se programska oprema projektirati i izrađivati prema osobinama radnika koji obavljaju određeni posao, nego prema zahtjevima radnog mjesta. Također, upitno je kako će poslodavac primijeniti načela da «programska oprema mora zadovoljavati ergonomske zahtjeve, posebno pri obradi podataka» ili da «sustav mora radniku davati povratne informacije o izvođenju njegovih radnih zadaća», jer su navedena načela preopćenita, te time ostavljaju prostor za različita tumačenja. Smatramo da je samo posljednje načelo navedeno u pravilniku, a koje se odnosi na boju slova i zaslona, jedino koje poslodavac može pri izboru programske opreme nedvojbeno prepoznati i poštovati.

Prilog pravilniku su zahtjevi koje mora ispunjavati radno mjesto, a poslodavcima je dan rok od četiri godine za zamjenu postojeće opreme i namještaja. Stoga se danas rijetko može pronaći tvrtka koja vodi računa o ergonomskim zahtjevima koje mjesta za rad s računalima trebaju zadovoljavati. Pozitivan primjer je Ericsson Nikola Tesla gdje su problemi prepoznati još 2003. godine i gdje se sustavno provodi zaštita djelatnika pri radu s računalom[18]. U nekim tvrtkama su započete aktivnosti na analizi i unapređenju postojećeg stanja, međutim najčešće financijske mogućnosti tvrtke značajno ograničavaju primjenu mjera zaštite. Stoga nije rijetkost da su radna mjesta s računalima smještena u neadekvatnom i nepravilno osvijetljenom prostoru, da zaposlenici nemaju dovoljno prostora za rad, da radni stolovi i stolci nisu prilagođeni tjelesnim osobinama zaposlenika, a često nisu niti namijenjeni za rad za računalom i slično. U takvim okolnostima poželjno je barem educirati zaposlenike o organizaciji odmora i vježbi tijekom duljeg rada s računalom (danas je uobičajeno raditi na računalu puno dnevno radno vrijeme, a i dulje), te inzistirati na preventivnim zdravstvenim pregledima zaposlenika. Radno mjesto po mjeri zaposlenika povećava radne učinke jer zaposlenik može raditi brže, bolje i efikasnije (i točnije). Stoga stručnjaci za zaštitu na radu moraju mjere koje se odnose na radna mjesta s računalima uključiti u sigurnosnu politiku za zaštitu informacijskog sustava tvrtke.

Zaposlenike je moguće i dodatno zaštititi i sklapanjem odgovarajuće police osiguranja kojom se omogućava besplatna dodatna zdravstvena zaštita, koja uključuje i preventivne preglede[19]. Nažalost, zakonska regulativa u Hrvatskoj je nepovoljna za poslodavce koji zaključuju takve police za svoje zaposlenike, tako da samo mali broj tvrtki ulaže u ovaj oblik zaštite.

ZAKLJUČAK

Unatoč svakodnevnoj uporabi računala, veliki broj tvrtki ne primjenjuje zaštitu informacijskih sustava u poslovnoj praksi. Međutim, porast broja zloporaba informacijske tehnologije i neminovnost uvođenja mjera zaštite na radu za radna mjesta s računalima utjecat će na poslodavce da izaberu neki od modela zaštite informacijskih sustava.

[18] Prema Lipnjak, G. i Pap, Z.: Primjena upitnika o ergonomskim aspektima rada za računalom, Rad i sigurnost, 3-2003., str. 223- 231.

[19] Vjerojatnost nezgode na radu kod radnih mjesta s računalima je zanemariva.

Model organizacije uz primjenu pravilnika o zaštiti informacijskog sustava proizišao je iz prakse i u njegovom oblikovanju sudjelovali su i informatičari i druge stručne službe u poduzećima. Zaposlenicima je prepoznatljiv jer je osnovna konstrukcija slična ostalim pravilnicima koji se primjenjuju u praksi.

Model organizacije uz primjenu norme ISO/IEC 17799:2000 (odnosno BS 7799) opisan je općenitije, pa omogućava interpretaciju pojedinih poglavlja sadržaja prema potrebama tvrtke koja ga primjenjuje. Za sada je samo jedna tvrtka u Hrvatskoj uspjela proći zahtjevan postupak usklađivanja sigurnosnih pravila informacijskog sustava s normom BS 7799-2 te je dobila certifikat za informacijsku sigurnost.

Oba modela omogućavaju dopunu posebnim mjerama zaštite na radu na radnim mjestima s računalima koje su propisane Pravilnikom o sigurnosti i zaštiti zdravlja pri radu s računalom, te ističu timski rad stručnjaka različitih profila na izradi i primjeni potrebnih dokumenata i procedura. Sigurnost informacijskog sustava na taj način postaje dio izgradnje cjelovitog sustava sigurnosti u tvrtki.

LITERATURA

Klasić, K. i Klasić, I.: Dva modela organizacije zaštite informacijskog sustava/Two Models of Organizing Information System Protection, *Rad i sigurnost,* br. 3-2002, str. 213-234.

Klasić, K: *Zaštita informacijskih sustava,* IPROZ, Zagreb, 2002.

Klasić, K.: Organizacija zaštite informacijskih sustava, *Suvremeno poduzetništvo,* br. 5, str. 80-88, 2003.

Krakar, Z.: Sustavi sigurnosti u informatici kao dio kvalitete sustava, *Savjetovanje CASE 13,* Opatija, 2001.

Lipnjak, G. i Pap, Z.: Primjena upitnika o ergonomskim aspektima rada za računalom, /Application of the Questionnaire on the Ergonomic Aspect of Working at the Computer, *Rad i sigurnost,* 3-2003, str. 223-231.

Nacionalni program informacijske sigurnosti u RH, www.e-hrvatska.hr, 2005.

Panian, Ž.: *Kontrola i revizija informacijskih sustava,* Sinergija, Zagreb, 2001.

Pravilnik o sigurnosti i zaštiti zdravlja pri radu s računalom, N.N., br. 69/05.

www.dnv.hr, 26.02.2006.

www.isaca.com (Information Systems Audit and Control Association)

www.vlast.net, 23.05.2005.

Zebec Koren, M. i Ključevšek, R.: Sustav upravljanja informatičkom sigurnošću, *Svijet osiguranja,* br. 5/2001.

INFORMATION SYSTEM SECURITY IN BUSINESS PRACTICE

SUMMARY: The application of information technologies in daily work is marking an ever-increasing trend. Only ten years ago a relatively small number of employees used a computer in their work, whereas it is nowadays unthinkable that a person without computer skills would get employment. The number of hours spent in active work at the computer is growing and not only in companies with business in information. One of the consequences is that occupational safety experts are constantly and increasingly faced with a range of problems arising from the application of the computer in business practice which directly or indirectly affect work results.

Each company has its own information system that may or may not be supported by a computer. It may, however, be asserted that information technology has penetrated all pores of business and everyday life resulting from, to a great degree, a decentralization of equipment and software. In the process, more often than not, no suitable protection of computers and data has been designed, and the existing regulations applied in centralized computer centers are not regularly updated. The introduction of the Internet technology only compounds the insecurity of information systems. The users of an information system or one of its segments are occasionally not even aware of the need and importance of the data resources in a company and the methods for their protection. Data is the fundamental resource of a company, so that damage stemming from their abuse (loss, misuse, etc.) is harmful to the company as a whole. Therefore the organization of information system security is an interdisciplinary task involving all employees in a company with the aim to ensure as high as possible security, but with awareness that some losses are acceptable and need to be tolerated. For this purpose a variety of documents is used relevant to the different aspects of system security, which are by and large introduced only after some compromise in the system security has been observed. In practice, the obligation to compile and implement such documents is commonly prescribed by a special set of regulations, with only very few companies introducing a model of information system security which is in compliance with the international ISO/IEC 17799:2000 standard.

Furthermore, the protection of employees working at the computer on a daily basis in their jobs must also be regulated in the Safety and Health Regulations in Working with Computers. The Regulations prescribe the requirements which the computer equipment must comply with, with a mandatory risk assessment for the work places.

Information system security is the responsibility of all employees in a company. Only healthy, happy and suitably trained employees working in satisfactory working conditions may contribute to the improvements in equipment and data security in a business system.

Key words: *information system, information system security, occupational safety, ergonomics, ISO/IEC 17799:2000, Safety and Health Regulations in Working with Computers*

Professional paper
Received: 2006-03-08
Accepted: 2007-01-04