8 UPRAVLJANJE IN VAROVANJE INFORMACIJSKIH VIROV

Ko boste prebrali poglavje, boste:

- znali opredeliti informacijske vire podjetja ter način priskrbe informacijskih virov
- poznali vlogo informatike v podjetju ter njen razvoj skozi leta
- poznali nevarnosti, ki pretijo informacijskim virom
- poznali namerno in nenamerno ogrožanje informacijskih virov
- poznali načine varovanja informacijskih virov podjetja
- poznali načine zavarovanja podatkov pri e-plačevanju.

8.1 Informacijski viri in informatika

Spoznali smo, da s pomočjo informacijskega sistema zajemamo, obdelujemo, hranimo in posredujemo podatke, ki jih uporabniki pretvorijo v informacije. IS je torej vir informacij, zaradi česar so sestavine IS informacijski viri podjetja. **Informacijski viri** so torej IKT (strojna in programska računalniška oprema ter računalniška omrežja), podatki, postopki in ljudje (Rainer in Turban 2009, 48). Vsi ti viri so za podjetje vir pridobivanja strateške prednosti pred konkurenco, zato je informacijske vire potrebno upravljati – priskrbeti, uporabljati in vzdrževati.

V poglavju o informatizaciji poslovanja smo spoznali, da podjetje programske rešitve lahko pridobi na različne načine:

- prilagodi obstoječe programske rešitve,
- kupi ali najame standardizirane rešitve na trgu,
- nove programske rešitve razvije samo,
- razvoj in uvedbo računalniških rešitev zaupa zunanjim izvajalcem (angl. Outsourcing).

Strojno in telekomunikacijsko opremo podjetje lahko kupi ali pa najame. V poglavju o informacijski infrastrukturi smo že srečali inovativno rabo strojne opreme, ki podjetjem z razpoložljivo IKT opremo omogoča racionalno izrabo obstoječih zmogljivosti in vzporedno dodatne zaslužke, podjetjem, predvsem manjšim, brez ustrezne infrastrukture pa ekonomsko upravičen najem kapacitet. Upravljanje z informacijskimi vir je potrebno ne glede na način njihove pridobitve. Za informacijske vire lahko skrbijo *končni uporabniki sami* (angl. End-user computing), ali pa **služba za informatiko**, katere vloga se je skozi leta spreminjala. Od začetne *Službe za avtomatsko obdelavo podatkov* (službe AOP), ki je bila večinoma odgovorna za obdelavo podatkov, do *Službe za informatiko*, ki skrbi za vzpostavljanje IKT infrastrukture, vzdrževanje opreme, podporo in usposabljanje uporabnikov ter za razvoj, vpeljavo in vzdrževanje IS. Sodobno organizirano službo za informatiko vodi vodja službe, ki ga v praksi zasledimo tudi s kratico CIO (angl. Chief Information Officer). Glede na pomen, ki jo ima informatika za strateški razvoj podjetja – ne pozabimo, da informatika, kot podporna dejavnost, podpira doseganje strateških ciljev podjetja, naj bi vodja informatike bil ožji član uprave podjetja.

Zaposleni v službi za informatiko morajo imeti različna znanja, tako s področja računalništva,

kot znanja s področja poslovnih in organizacijskih ved. Brez poslovnega znanja bi informatiki težko uspešno podprli poslovne procese v podjetju. Uspešnega dela na področju informatike ni brez veščin timskega dela, komuniciranja, poznavanja postopkov vodenja projektov, zagotavljanja kakovosti idr. Služba za informatiko tako potrebuje strokovnjake s področij:

- programiranja
- vzdrževanja IKT opreme
- projektiranja IS
- sistemske analize
- skrbništva omrežij in strežnikov
- skrbništva spletnih rešitev
- skrbništva baz podatkov idr.

Podjetje lahko upravljanje informacijskih virov zaupa zunanjemu izvajalcu (podjetju ali posamezniku), ki vzdržuje infrastrukturo in programsko opremo, nudi pomoč uporabnikov, skrbi za razvoj itn. Takšne rešitve uporabljajo predvsem majhna podjetja, ki sama nimajo ustreznega znanja in kadrov, da bi lahko upravljala s svojimi informacijskimi viri.

8.2 Ranljivost IS in računalniški kriminal

Informacijski viri so razporejeni po podjetju v različnih oblikah, poleg tega pa se viri pogosto prenašajo – zaposleni potujejo s prenosnimi računalniki, pogosto jih prenašajo domov, da bi dokončali nedokončano delo. Informacije se prenašajo od in iz podjetja ter med samimi deli podjetja. Vedno več je tudi dela na daljavo, pri katerem zaposleni do IS podjetja dostopajo od kjer koli in kadar koli. Nevarnosti pretijo na vse informacijske vire: fizične vire informacijskega sistema (računalnike in drugo opremo), podatke, programe, procese itd. (Turban 2006, 641).

Večanje števila uporabnikov Interneta, predvsem pa razvoj IKT, ki omogoča brezžično povezavo[141] od kjer koli in kadarkoli, izpostavlja informacijske vire podjetij stalnim grožnjam. Dokler so podjetja poslovala prek zaprtih varnih omrežjih (VAN omrežja), je bilo teh nevarnosti veliko manj. Danes pa lahko, tako posamezniki kot podjetja, do Interneta dostopijo tudi prek številnih brezžičnih, prosto dostopnih, omrežij. Ta omrežja so manj varna in tako bolj ranljiva. Na trgu se pojavljajo tudi številna orodja (programi), ki omogočajo enostaven vdor v računalnik, tudi brez posebnega računalniškega znanja.

Pomnilni mediji, ki jih uporabljamo pri vsakodnevnem delu so po velikosti vse manjši, hranijo velike količine podatkov, so prenosljivi... s čemer se poveča ranljivost podatkov shranjenih na teh pomnilnikih. Zaradi nižjih cen IKT opreme, je le-ta dostopna vsakomur, kakor je dostopen tudi Internet.

Kot smo videli so informacijski viri različni – strojna in programska oprema, omrežja in omrežna oprema, baze podatkov in podatki, postopki in ljudje. Vsi ti viri so ranljivi in izpostavljeni različnim nevarnostim. Te so lahko povzročene namerno ali nenamerno. Informacijske vire lahko ogrožajo zaposleni ali pa grožnje prihajajo od zunaj.

Nenamerne povzročene grožnje pogosto prihajajo zaradi napačnega ravnanja **zaposlenih** –

[141] Zavedati se moramo, da so številna brezžična omrežja nevarovana, kar pomeni, da so podatki, ki se pretakajo po teh omrežjih na udaru vsem, ki želijo podatke ukrasti ali pa podjetjem na kakršen koli drugi način škodovati.

npr. premalo usposobljeni uporabniki, ki vnašajo napačne podatke, ali pa pri svojem delu uporabljajo neprimerna gesla, oziroma nepravilno rokujejo z njimi, in tako povzročajo napake ali pa sistem naredijo ranljiv – vsak, ki pozna geslo za vstop do sistema, lahko vstopi, podatke doda, briše ali kako drugače spremeni. Grožnje IS ne predstavljajo le redno zaposleni, temveč tudi npr. pogodbeno zaposleni delavci ali strokovnjaki, ki s podjetjem (začasno) sodelujejo na določenem projektu. Pri zagotavljanju varnosti IS se pogosto pozablja na osebe, ki npr. skrbijo za čiščenje ali varovanje prostorov. Tudi te **osebe** imajo dostop do vseh prostorov in s tem do IKT opreme. Čistilka lahko, na primer, čisto po nesreči, med čiščenjem, izključi napajanje računalnika, ravno, ko se izdeluje zaščitna kopija podatkov. Izpad elektrike lahko povzroči napake pri zapisu podatkov na disk, ipd.

Med nenamerne grožnje uvrščamo tudi **nesreče**, kot so na primer poplave, potresi, požari ipd. Informacijske vire ogrožajo tudi razmere v prostorih, kjer se viri nahajajo – npr. prah in umazanija, statična elektrika, vlaga, previsoka temperatura, ipd.

Grožnjo informacijskim virom predstavlja tudi nekakovostno izvajanje informacijske dejavnosti s strani zunanjega izvajalca. Pa ne samo nekakovostno delo, tudi izpad omrežja ali električne energije ogroža informacijske vire podjetja.

Težave z delovanjem IKT opreme so lahko posledica napak v opremi, tako strojni kot programski opremi.

Težave pri delovanju IS so lahko vezane tudi z nerazumevanjem vodstva glede potreb po zagotavljanju varnosti. Varovanje informacijskih virov namreč zahteva denarna sredstva, katerih vir mora zagotoviti vodstvo podjetja. Brez razumevanja vloge informatike v podjetju in pomena informatike za strateški razvoj podjetja, vključno z varnostnim vidikom informacijskih virov, bodo potrebna sredstva (in tudi kadri) težko zagotovljena.

Informacijski viri so izpostavljeni tudi **namernim grožnjam**. Če bi nenamerne grožnje lahko opredelili kot nesreče oziroma dejanja, ki jih posamezniki niso hoteli storiti, pa so namerne grožnje storjene iz različnih namenov. Posamezniki, ki vdirajo v sistem lahko to počnejo z namenom pridobivanja podatkov, povzročanja izpada sistema konkurenčnega podjetja, ali pa samo izkazovanja ranljivosti sistema.

Zanimiv način, kako priti do informacijskih virov je **socialni inženiring**, ki socialne stike izkorišča za pridobitev zaupnih podatkov, kot je na primer uporabniško ime in geslo, s katerim je možno priti do IS in podatkov. Tako se npr. lahko nekdo predstavi za vzdrževalca IKT opreme, ki preverja – osebno ali po telefonu, delovanje IS, zato prosi zaposlenega, da mu pove uporabniško ime in geslo za dostop do informacijskih virov (intraneta, IS, podatkov itn). Zaposleni v dobri veri, da pomaga rešiti težave, v katerih se je podjetje znašlo, podatke zaupa in s tem vsiljivcu nehote omogoči dostop do informacijskih virov podjetja. Zato je potrebno zaposlene opozoriti, da se podatke ne izdaja nepooblaščenim osebam, oziroma je njihovo identiteto in pooblastila za opravljanje določene dejavnosti potrebno preveriti. Oseba, ki nepooblaščeno dostopi do informacijskih virov (lahko tudi na daljavo), lahko na računalnik naloži zlonamerno kodo, ki na primer zbira tudi druga gesla uporabnikov računalnika, vključno z gesli, ki so potrebna za opravljanje finančnega poslovanja.

Posamezniki ali podjetja poskušajo vdreti v druge IS za pridobitev podatkov, ki podjetju prinaša konkurenčno prednost, ali zaradi t. i. industrijskega vohunstva. V primeru konkurenčne prednosti

lahko niti ne gre za vdore, temveč za podrobno študijo spletne strani, da bi ugotovili, kje bi lahko bili vzroki za konkurenčno prednost podjetja. V primeru industrijskega vohunstva pa posamezniki ali podjetja uporabljajo prijeme, ki presegajo legalno dovoljene meje (npr. vdor v IS, lahko tudi s pomočjo socialnega inženiringa).

Opozorili bi radi na krajo podatkov, kot so npr. podatki o kupcih, ki se jih potem prodaja naprej, tretjim osebam.

Pri **sabotaži** in **vandalizmu** gre pogosto za vdor na spletno mesto, kjer vdiralec, namesto spletne strani podjetja, postavi povezavo na drugo spletno stran, ki lahko smeši podjetje, ali pa poslovanje, ki poteka prek spletne strani preusmeri drugam.

Seveda nevarnost za informacijske vire predstavljajo tudi **fizični vdori v prostore**, kjer se informacijski viri nahajajo – kraja, uničenje itn.

Internet ni zanimiv le za druženje in poslovanje, temveč postaja zanimiv tudi za kriminalne dejavnosti. Tako se na splet širi nelegalna dejavnost, ki jo poznamo pod imenom **računalniški (spletni) kriminal**. Pojavlja se tudi pojem »cyber« kriminal (angl. Cyber-crime). Spletni kriminal se lahko izvaja na različne načine: računalniki so lahko *tarča* kriminala, lahko so *orodje* za izvajanje napada ali se uporabljajo *za zavajanje žrtev*. Računalniški kriminal lahko izvajajo ljudje znotraj ali zunaj podjetja. Zunanji kriminalci ponavadi za kriminalna dejanja izkoriščajo komunikacijske linije, notranji kriminalci (zaposleni) pa ponavadi izkoriščajo svoj dostop do sistema v podjetju. Po ameriških podatkih so najbolj verjetni viri napadov na ameriška podjetja: neodvisni zunanji napadalci (82 %), nezadovoljni zaposleni (78 %), domači konkurenti (40 %), tuje vlade (28 %) in tuja podjetja (25 %). Iz teh podatkov je razvidno, da presenetljivo veliko napadov izvira znotraj podjetja. Tudi zunanji napadalci pogosto zlorabijo zaupanje zaposlenih za dostop do pomembnih informacij. (Turban 2006, 647–648)

Računalniške zlorabe v številkah (Haag in Cummings 2012, 245)

• Izgube zaradi računalniške goljufije (svet v letu 2009)	2,9 trilion USD
• Povprečni strošek goljufije	160.000 USD
• Delež goljufij, ki jih povzročijo zaposleni	42 %
• Delež goljufij, ki jih povzroči managerji	41 %
• Delež goljufij, ki jih povzročijo lastniki podjetja	17 %
• Čas, ki ga lastnik potrebuje, da odkrije goljufijo	24 mesecev
• Delež moških storilcev	67 %

Pogosta oblika računalniškega kriminala so programski napadi, ki lahko prizadenejo podjetja in posameznike. Metode programskih napadov na računalniške sistem so recimo:

- **Virusi** – so najbolj pogosta metoda napada, škodo pa povzročijo tako, da se prilepijo na obstoječ program brez vednosti uporabnika (določen program »okužijo«) (Turban 2006, 649–650). Ko uporabnik požene okužen program, omogoči virusu širjenje in povzročanje škode tako na okuženem programu kot na drugih programih (prav tam). Virus lahko tako npr. briše datoteke ali celo poškodujejo disk. Virusi, kot gostitelja, lahko uporabijo datoteke

različnih formatov (ne samo .exe, ampak tudi .doc, .xls). Čeprav so virusi zelo pogosti in nevarni, si je potrebno zapomniti, da je za izvršitev virusa vedno potrebna določena akcija na strani uporabnika (npr. odpiranje priponke pri e-pošti).

- **Črvi –** so posebna vrsta virusov, ki se širijo preko računalniških omrežij. Črvi za delovanje ne potrebujejo programa gostitelja, saj se znajo sami razmnoževati in širiti. (Turban 2006, 649)
- **Trojanski konj –** je ilegalni del oziroma skrita funkcija določenega programa. Ob uporabi takega programa se hkrati izvrši tudi skrita funkcija, s katero uporabnik ni seznanjen, mu pa povzroči škodo. (prav tam)
- **Stranska vrata** (angl. Trap Door) – omogočajo vdor v program in njegovo spreminjanje brez vednosti uporabnika. Stranska vrata nehote ali hote v programe vgradijo programerji. (prav tam)
- **Ohromitev strežnika** (angl. Denial of Service), kjer napadalec strežnik zasuje s podatkovnimi paketki in posledično ohromi njegovo delovanje, saj ima določen strežnik na voljo omejene vire za procesiranje zahtev (to izhaja iz modela odjemalec/strežnik, ki smo ga opisali v 2. poglavju). (prav tam)
- **Vohljači** (angl. Sniffers) – so programi, ki pregledujejo podatkovne paketke, ki potujejo po Internetu in iščejo geslo ali določeno vsebino. (prav tam)
- **Sleparjenje** (angl. Spoofing), kjer t. i. sleparji ponaredijo e-poštni naslov ali spletno stran z namenom, da bi od uporabnikov zbrali pomembne podatke ali denar.[142] (prav tam)
- **Razdiralec gesel** (angl. Password Cracker) je program, ki poskuša ugotoviti geslo uporabnika. Pri tem so lahko zelo uspešni, saj večina uporabnikov uporablja nezahtevna gesla, ki so sestavljena iz imen ali navadnih besed.[143] (prav tam)
- **Zlonamerna koda** (angl. Malicious Applets) predstavlja programe napisane v programskem jeziku Java, ki lahko povzročijo zlorabo računalniških virov, spreminjanje datotek, pošiljanje e-pošte ipd.. (prav tam)

Glede na to, da je nevarnostim izpostavljeno veliko različnih informacijskih virov, ne preseneča, da je seznam možnih nevarnosti, ki lahko ogrozijo informacijske vire, obsežen. Whitman (2003, 92) jih v splošnem razdeli v 12 kategorij:

- **Človeške napake** (nesreče, napake zaposlenih),
- **Nespoštovanje intelektualne lastnine** (piratstvo, kršitve avtorskih pravic),
- **Namerna dejanja vohunstva ali prestopa** (neavtoriziran dostop in/ali zbiranje podatkov),
- **Namerna dejanja izsiljevanja informacij** (grožnje ali izsiljevanja z razkrivanjem informacij),
- **Namerna dejanje sabotaže ali vandalizma** (uničenje sistemov ali informacij),
- **Namerna dejanja kraje** (nelegalen zaseg opreme ali informacij),
- **Namerni programski napadi** (virusi, črvi ipd.),
- **Naravne sile** (požar, poplava, potres, udarci strele),
- **Kakovost na strani ponudnikov storitev** (kakovost električnih in omrežnih storitev),

[142] Pred sleparjenjem nismo varni tudi v Sloveniji. Nedavna žrtev sleparjenja je bila recimo NLB (več o tem na: http://www.nlb.si/cgi-bin/nlbweb.exe?doc=16038).

[143] Več o varnih geslih na: http://www.getsafeonline.org/nqcontent.cfm?a_id=1127.

- **Tehnične odpovedi ali napake pri strojni opremi** (odpoved opreme),
- **Tehnične odpovedi ali napake pri programski opremi** (hrošči, razni problemi v programski kodi),
- **Tehnološka zastarelost** (zastarane tehnologije).

8.3 Varovanje informacijskih virov

Kot vidimo je nevarnosti pri uporabi informacijskih virov precej. Vendar se pred vsemi temi nevarnostmi možno zavarovati. Da bi zmanjšali ogroženost informacijskih virov, moramo **s tveganji upravljati,** kar pomeni, da jih moramo prepoznati, nadzirati in ravnati tako, da zmanjšamo tveganje (Rainer in Turban 2009, 80). Upravljanje tveganj (angl. Risk management) vključuje tri procese – ocena tveganja, zmanjšanje tveganja in vrednotenje varovanja (prav tam). Pri oceni tveganja (Turban idr. 2002, 549; Rainer in Turban 2009, 80) mora podjetje **oceniti tveganje** za fizično (računalniški sistem, omrežja) in nefizično (nevidno premoženje) premoženje (npr. načrti, podatki o kupcih, gesla, digitalni podpis). Varovanje informacijskih virov mora biti stroškovno učinkovito, kar pomeni, da so stroški varovanja primerljivi z ocenjenimi stroški, ki bi nastali zaradi ranljivosti informacijskih virov.

Podjetje mora sprejeti **ukrepe za zmanjšanje tveganja**, zato mora načrtovati politiko varovanja in uvesti varovalne ukrepe. **Izvajanje politike varovanja** mora podjetje spremljati in vrednotiti, ter po potrebi dopolnjevati.

En najstarejši oblik varovanja informacijskih virov je **fizično varovanje**, kar pomeni, da podjetje varuje dostop do opreme. To lahko naredi z zaklepanjem opreme v zaprte prostore, namestitvijo alarmne naprave, varovanje s pomočjo varnostnikom ipd. Vstop v zaprte proste se omeji le osebam, ki imajo dovoljenje za dostop in se na ustrezen način identificirajo (različni ključi – npr. magnetne kartice, biometričen način identifikacije ipd). Način dostopa do informacijskih virov mora podjetje opredeliti v politiki varovanja.

Za varnost lahko torej poskrbimo z različnimi **programskimi in strojnimi rešitvami**. Pri dostopu do informacijskih virov ločimo **pooblastilo** (dovoljenje za dostop) in **identifikacijo** osebe (prepoznavanje osebe), ki bi želela dostopiti do informacijskih virov. Identifikacija se vrši na več načinov:

- z nečem, *kar oseba je*, kar poznamo kot biometričen način identifikacije, ki preveri fizične značilnosti osebe (npr. prstni odtis ali preslikava očesa),
- z nečem, *kar oseba ima* – na primer identifikacijsko kartico s sliko ali pametno elektronsko kartico,
- nekaj, *kar oseba naredi* – npr. oseba pove skrivno geslo, oseba se podpiše,
- nekaj, *kar oseba ve* – npr. vnos gesla. Zaposleni pogosto uporabljajo slaba gesla – npr. za geslo uporabijo imena otrok, partnerja, prijateljev, glasbene skupine, športnega kluba, domačih živali ipd. Ali pa, sicer dobra oz. močna gesla, hranijo na vidnem mestu, tako da do gesel lahko pride vsakdo in na takšen način vstopi v IS in zlorabi podatke ali pa povzroči napačno delovanje IS. **Močna gesla** (Rainer in Turban 2009, 83):
  - naj bodo takšna, da jih je težko uganiti,
  - naj bodo daljša, naj vključujejo kombinacijo malih in velikih črk, številk in posebnih

znakov,
- ne uporabljamo prepoznane besede, ali besede, ki so povezani z nami (imena oseb ali domačih ljubljenčkov, datumi rojstev ipd).

Seveda lahko uporabimo tudi kombinacijo različnih načinov – recimo oseba nekaj ima, nekaj ve in nekaj naredi.

Podjetje na različne načine varuje prenos podatkov po omrežjih. Pogost način varovanja je t. i. **požarni zid** (angl. Firewall), ki preprečuje neavtoriziran vstop na računalnik oziroma v omrežje podjetja. Problematičen je predvsem pretok podatkov iz javnih omrežij na zasebna omrežja. Naloge požarnega zida lahko izvaja strojna ali programska oprema, ali pa požarni zid postavimo s kombinacijo strojne in programske opreme. Podjetja lahko uporabljajo tudi dva požarna zida – zunanjega in notranjega, ki varuje intranet podjetja. Med obema požarnima zidoma je t. i. demilitarizirana cona. Takšen način se uporablja tako za spletne strani kot e-pošto.

Pred zlonamerno kodo se podjetje zaščiti s t. i. antivirusno zaščito, ki vključuje programsko opremo za odkrivanje in odstranjevanje virusov, črvov, trojanskih konjev in druge zlonamerne kode. Najbolj poznana sta Nortonov[144] in McAfee[145] antivirusna programa. Za domačo rabo je uporaben antivirusni program AVG,[146] ki ga je, za domačo rabo, brezplačen.

Znova je pomembno poudariti, da je potrebno varnostno strategijo pazljivo načrtovati in poskrbeti, da jo zaposleni poznajo in tudi upoštevajo. Nenazadnje je pomembno, da imajo podjetja načrte tudi za primere nesreč, odpovedi strojne in programske opreme, napak ali vdorov, saj se pred vsemi nevarnostmi nikoli ne moremo popolnoma obvarovati (npr. primer naravne nesreče). Zato je pomembno, da podjetja izdelujejo **varnostne kopije** pomembnih podatkov[147] (angl. Backup). Varnostne kopije se lahko nahajajo na rezervnih strežnikih, v določeni primerih tudi na drugi lokaciji.

8.4 Varnost pri elektronskem plačevanju

Varnost je še posebej pomembna pri elektronskem plačevanju. Pri varnem e-plačevanju morajo biti izpolnjene naslednje varnostne zahteve: (Turban 2006, 168)

- **Avtentikacija**: kupec, prodajalec in plačilni posredniki morajo biti prepričani o identiteti vseh sodelujočih v procesu e-plačevanja;
- **Integriteta**: zagotoviti je treba, da se podatki o naročilu ipd. ne spremenijo ali izgubijo med prenosom;
- **Neizpodbitnost**: prodajalci potrebujejo zaščito pred neutemeljenim zanikanjem naročila s strani kupca, kupci pa potrebujejo zaščito pred neutemeljenim zanikanjem plačila s strani prodajalca;
- **Zasebnost**: veliko kupcev želi pri kupovanju zasebnost, kar pomeni, da ne želijo, da bi ostali izvedeli, kaj kupujejo;
- **Varnost**: kupci morajo vedeti, ali je varno posredovati številko kreditne kartice preko

[144] Http://www.symantec.com/index.jsp

[145] Http://www.mcafee.com/us/

[146] Http://www.avg.com/eu-en/home-small-office-security

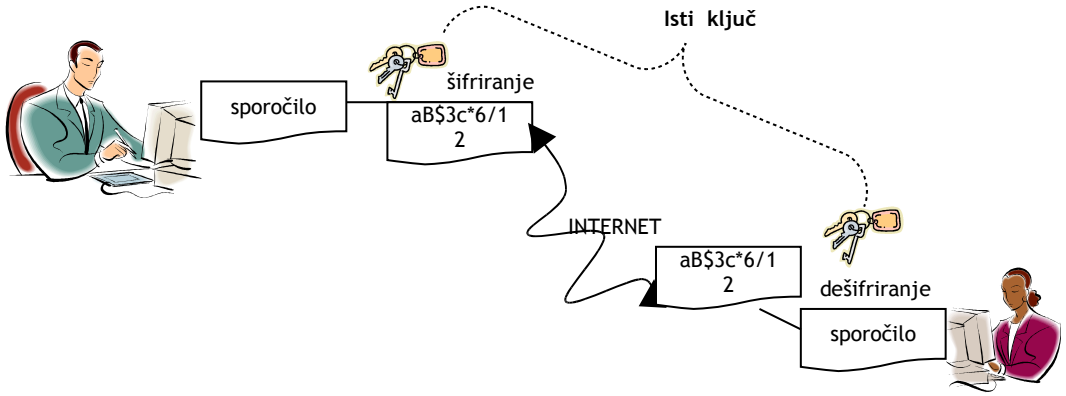
[147] Slednje je pogosto pomembno tudi za osebno rabo računalnikov. Varnostne kopije pomembnih dokumentov lahko recimo shranite na Internetu, zapečete na CD ipd..

Interneta. Prav tako želijo biti zaščiteni pred prevarami iz strani prodajalcev.

Zelo pomembno je torej, da zagotovimo **varen in verodostojen prenos podatkov** o naročilih in plačilih preko Interneta. Za varen način pošiljanja podatkov lahko uporabljamo sistem šifriranja podatkov in sicer **sistem enojnega (simetričnega)** ali **sistem dvojnega (asimetričnega) šifriranja**.

Poglejmo, kako s pomočjo šifriranja poskrbimo za varnost in zasebnost. Denimo, da Janez želi Metki poslati sporočilo, vendar ne želi, da bi to sporočilo prebral še kdo drug. Zato Janez svoje sporočilo šifrira. **Šifriranje sporočila** (angl. Encryption) je proces, s katerim sporočilo spremenimo v, širši javnosti, nerazumljivo zaporedje znakov in simbolov.

Slika 42: Šifriranje sporočil – sistem enojnega ključa



Povzeto po Turban idr. (1999, 261)

Tako šifrirano Janezovo sporočilo lahko razume le naslovnik (Metka), ki s pomočjo istega šifrirnega ključa šifrirano sporočilo spremeni v sporočilo, ki je identično izvirnemu sporočilu. Šifrirano sporočilo brez ustreznega ključa ni razumljivo. Seveda takoj pomislimo na možnost, da se šifrirni ključ izgubi ali pa zanj izvedo nepooblaščene osebe. V prvem primeru šifriranega sporočila ne bomo mogli prebrati oziroma razumeti, v drugem primeru pa sporočilo ni več zaupno, kar smo z uporabo šifrirnega ključa želeli doseči. **Sistem enojnega ključa** zagotavlja **zaupnost**, ne zagotavlja pa **prepoznavnosti** pošiljatelja in prejemnika sporočila. Način simetričnega šifriranja je sicer zelo hiter, vendar, če bi želeli na takšen način šifrirati sporočila pri e-poslovanju bi potrebovali veliko število ključev. Sama dolžina ključa ima pri varnosti velik pomen. Pomislite, koliko časa potrebujete, da uganete npr. 4-mestni ključ ključavnice na kolesu? Če bi bila številka večja, bi seveda potrebovali dalj časa. Z dolžino ključa[148] narašča njegova varnost. Zavedati se moramo, da se z razvojem zmogljivosti računalnikov in ustrezne programske opreme, povečuje zahteva po uporabi daljšega ključa, saj je kratek ključ možno hitro uganiti.

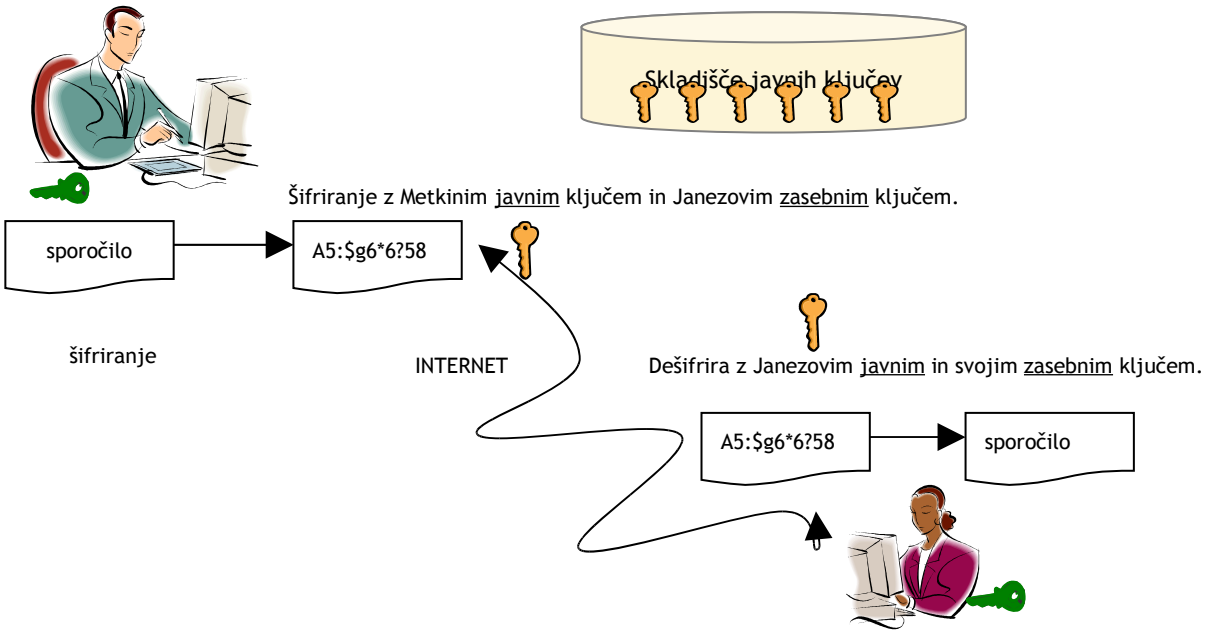
Za rešitev problemov, povezanih s sistemom enojnega ključa, se je razvil **sistem dvojnega šifriranja**, ki vključuje javni in zasebni ključ. Poglejmo primer.

Janez pošlje Metki sporočilo in želi, da ga prebere samo Metka. Tako Janez svoje sporočilo šifrira s svojim zasebnim ključem in z Metkinim javnim ključem. Da bi nekdo sporočilo prebral in razumel, potrebuje ustrezen ključ. V tem primeru potrebuje Metka Janezov javni ključ, kar pomeni, da bo Janezova sporočila lahko brala le, če ji bo Janez poslal sporočilo, ki ga je šifriral s svojim zasebnim ključem. Ker je Janez želel, da sporočilo prebere samo Metka in ga je šifriral z Metkinim

[148] Več o dolžini ključa: http://www.si-ca.si/kripto/dolz-klj.htm.

javnim ključem, lahko le Metka s svojim zasebnim ključem odpre sporočilo in prebere vsebino.

Slika 43: Šifriranje sporočil – sistem dvojnega ključa

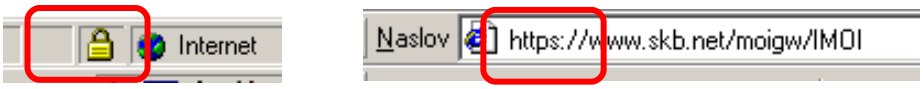


Kot vidimo, ključa za šifriranje in dešifriranje nastopata v paru – zasebni in javni ključ. Medtem ko so javni ključi javno dostopni, pa so zasebni ključi varovani pri lastniku zasebnega ključa. Sporočilo v sistemu dvojnega šifriranja je razumljivo le, če oba partnerja poznata svoj zasebni ključ in uporabljata, za omejitev branja zgolj na prejemnika, partnerjev javni ključ. Sporočilo, šifrirano z javnim ključem odpira zasebni ključ in obratno. Zasebni in javni ključ sta med seboj v zahtevnem matematičnem razmerju, vendar iz javnega ključa posameznika dejansko ni mogoče izpeljati posameznikovega zasebnega ključa. Glede na to, da je eden od ključev znan, javen, tak način dela imenujejo **infrastruktura javnih ključev** (angl. Public Key Encryption), ki vključuje dva dodatna termina, navedena po terminologiji zakona (ZEPEP): **elektronski podpis** (angl. Digital Signature) in **digitalno potrdilo** (angl. Digital Certificate). Če e-poslovanje primerjamo s papirnim poslovanjem, potem elektronski podpis predstavlja lastnoročni podpis, digitalno potrdilo pa lahko primerjamo z osebno izkaznico, s katero se identificiramo, da smo res oseba za katero se izdajamo. Najbolj znan izdajatelj digitalnih potrdil v Sloveniji je SIGEN-CA, ki izdaja potrdila za fizične osebe in SIGOV-CA, ki izdaja potrdila za pravne osebe. Obe vrsti potrdil sta overjeni pri Ministrstvo za pravosodje in javno upravo.[149] Digitalno potrdilo za e-poslovanje je moč dobiti tudi pri Pošti Sloveniji (Pošta®CA),[150] pri AC NLB (digitalno potrdilo, ki se uporablja pri Klik NLB)[151] in pri podjetju Halcom (HALCOM CA).[152] Od tujih izdajateljev pa je najbolj znan Verisign.[153]

[149] Http://www.si-ca.si/index.php
[150] Http://postarca.posta.si/
[151] Http://www.nlb.si/?doc=5458
[152] Http://www.halcom.si/
[153] Https://www.verisign.com/ts-sem-page/?sl=t31300225410000002&gclid=COSRpovkzrICFc1d3godGUIAQA

Sistem dvojnega (asimetričnega) šifriranja zagotavlja zaupnost, verodostojnost in prepoznavnost. Najbolj razširjen algoritem za generiranje asimetričnih ključev je RSA,[154] ki s pomočjo posebnih matematičnih formul ustvari ključe dolžine 1024 ali 2048 bitov. Ključi, ki se uporabljajo v asimetričnem šifriranju so daljši od simetričnih ključev. Pri B2C e-poslovanju se uporablja SSL protokol (angl. Secure Sockets Layer Protocol).[155] Protokol je razvil Netscape, vendar ga sedaj podpirajo tudi drugi brskalniki, kot npr. Internet Explorer (Chaffey 2002, 456). Uporabo SSL protokola prepoznamo tudi uporabniki, saj nam brskalnik pokaže ključavnico (npr. Internet Explorer, Firefox) ali ključ (npr. Netscape), ker so orodja za varno posredovanje podatkov prek Interneta že vključena v internetna orodja. Ko se povežemo na spletno stran, ki je podprta s SSL standardom, se protokol prenosa podatkov iz http://... spremeni v https://... (Slika 44).

Slika 44: Internet Explorer pri varni komunikaciji prek interneta



Omenimo še **SET protokol** (angl. Secure Electronic Transactions), ki predstavlja standard za asimetrično šifriranje sporočil e-poslovanja (sistem javnega ključa). Standard je razvil konzorcij pod vodstvom Mastercarda in Visa (Chaffey 2002, 457). SET protokol omogoča kupcu potrditev, da je prodajalec legitimen in obratno, prodajalec ima garancijo, da je kupec lastnik kreditne kartice, saj se mora kupec podpisati s svojim e-podpisom. E-certifikat prodajalca in e-podpis kupca sta dovolj močna garancija za varno poslovanje.

SET protokol je počasnejši od SSL protokola. Vendar ni to edina ovira, da SET protokol ni tako široko uporabljen, kot SSL protokol. Pri SET protokolu nastopijo težave pri izmenjavi ključev. Za posedovanje lastnega ključa, moramo na svojem osebnem računalniku imeti instalirane posebne računalniške rešitve. Posebne računalniške rešitve morajo biti nameščene tudi na strežniku. Prednost SET protokola je pa predvsem v tem, da se številka kreditne kartice ne shranjuje na strežniku.

Ponovimo:

- Opredelite informacijske vire. Na kakšen način jih podjetje lahko pridobi?
- Razmislite o prednostih in slabostih posameznega načina pridobivanja informacijskih virov.
- Kdo v podjetju skrbi za upravljanje informacijskih virov in kako se je njihova vloga spreminjala skozi zgodovino?
- Katera znanja se iščejo pri zaposlenih na področju informatike?
- Kje vidite potencialno ranljivost IS v podjetju?
- Pojasnite primere namernega in nenamernega ogrožanja informacijskih virov podjetja.
- Kaj razumete pod pojmom socialni inženiring ter kakšen je njegov namen?
- Na kakšen način lahko podjetje varuje svoje informacijske vire?
- Kakšne načine računalniške kriminalitete poznate?

[154] Več o tem na http://www.rsasecurity.com/rsalabs/rsa_algorithm/index.html.

[155] Več o tem na http://www.gov.si/tecaj/kripto/kr-ssl.htm.

- Na kakšen način lahko identificiramo uporabnika IS?
- Pojasnite problematiko gesel, ki jih uporabljamo pri dostopu do različnih informacijskih virov.
- Pojasnite asimetričen in simetričen način šifriranja podatkov.
- V čem je pomen digitalnega potrdila in elektronskega podpisa?
- Kako ugotovimo, da se podatki, ki jih vnašamo v obrazec na spletni strani prenašajo varno? Pojasnite.

UPORABLJENA LITERATURA

Rainer, R. Kelly in Efraim Turban. 2009. Introduction to Information Systems: Enabling and Transforming Business. 2nd Edition, International Student Version. John Wiley & Sons.

Turban, E., D. King, J. Lee, M. Warkentin, H. M. Chung. 2002. *Electronic Commerce – A Managerial Perspective*. New Jersey: Prentice Hall.

Turban, Efraim, Dorothy Leidner, Ephraim McLean, and James Wetherbe. 2006. Information Technology for Management: Transforming Organizations in the Digital Economy. 5th ed. Wiley.