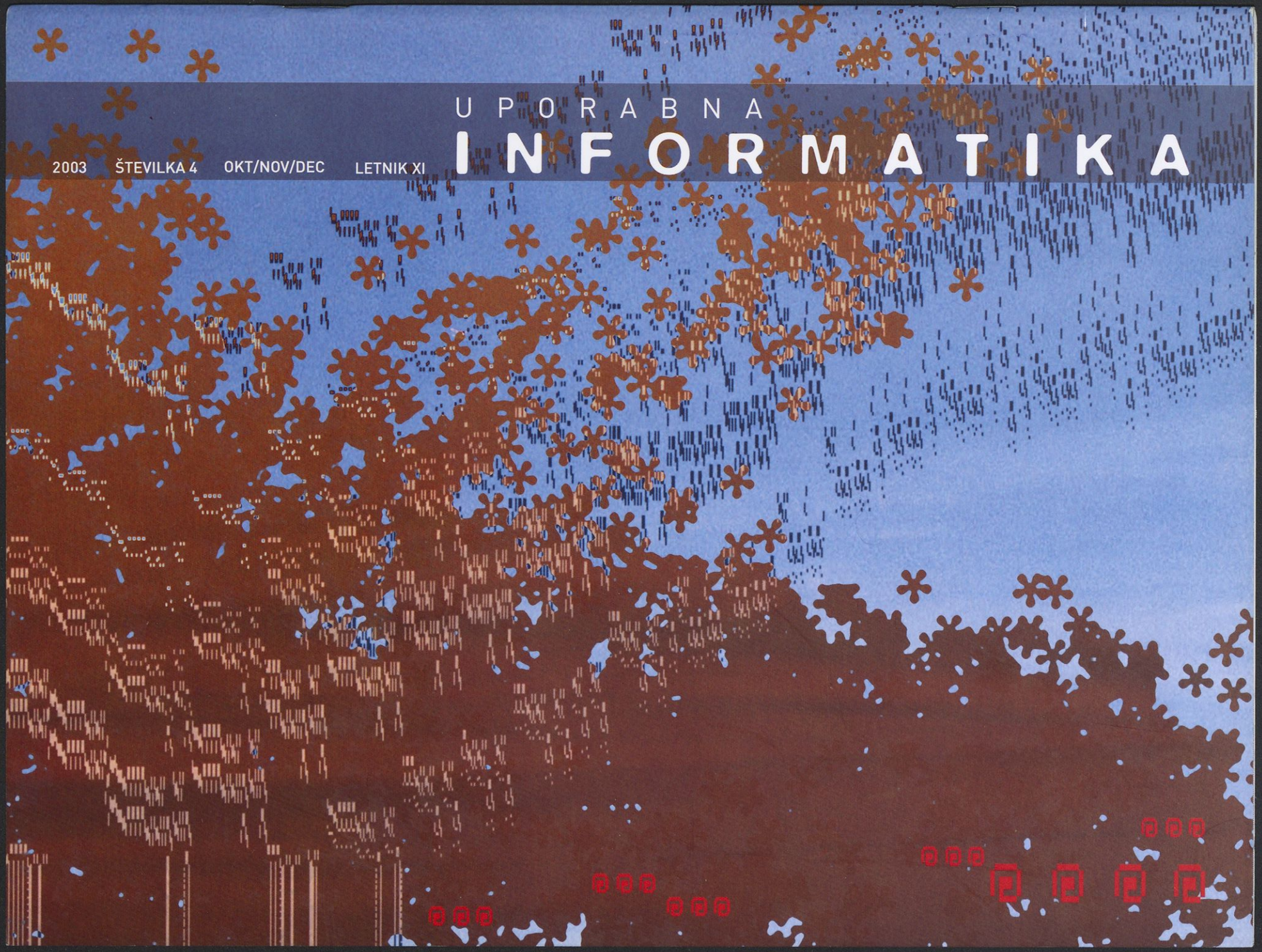
2003 ŠTEVILKA 4 OKT/NOV/DEC LETNIK XI

UPORABNA

INFORMATIKA



Testni centri ECDL

ECDL (European Computer Driving License), ki ga v Sloveniji imenujemo evropsko računalniško spričevalo, je standardni program usposabljanja uporabnikov, ki da zaposlenim potrebno znanje za delo s standardnimi računalniškimi programi na informatiziranem delovnem mestu, delodajalcem pa pomeni dokazilo o usposobljenosti. V Evropi je za uvajanje, usposabljanje in nadzor izvajanja ECDL pooblaščena ustanova ECDL Foundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics Societies) to pravico pridobilo Slovensko društvo INFORMATIKA. V državah Evropske unije so pri uvajanju ECDL močno angažirane srednje in visoke šole, aktivni pa so tudi različni vladni resorji. Posebej pomembno je, da velja spričevalo v več kot osemdesetih državah, ki so vključene v program ECDL. Doslej je bilo v svetu izdanih že več kot tri milijone indeksov, v Sloveniji okoli 1700 in podeljenih okoli tisoč spričeval. Za testne centre ECDL so se v Sloveniji usposobile organizacije, katerih logotipi so natisnjeni na tej strani.

AGORA ustvarjalne komunikacije

IZOBRAŽEVANJE INFORMACIJSKE STORITVE

ELES - ICES

e-trade Elit trade d.o.o. Zagreb

EUROCOM Simply logical

UNIVERZA V LJUBLJANI Fakulteta za pomorstvo in promet

ISA INFORMACIJSKE TEHNOLOGIJE

IVANUŠA Contact um

KOPA

LJUDSKA UNIVERZA KOPER
UNIVERSITÀ POPOLARE CAPODISTRIA

LJUDSKA UNIVERZA MURSKA SOBOTA

Micro Team

Much

spin

UPI LJUDSKA UNIVERZA ŽALEC
šola prijaznih ljudi

VLS computers

UPORABNA
INFORMATIKA
2003 ŠTEVILKA 4 OKT/NOV/DEC LETNIK XI ISSN 1318-1882

ISSN 1318-1882

Ustanovitelj in izdajatelj:
Slovensko društvo INFORMATIKA
Vožarski pot 12
1000 Ljubljana

Predstavnik
Niko Schlamberger

Odgovorni urednik:
Andrej Kovačič

Tehnična urednica
Mira Turk Škraba

Oblikovanje
Bons

Prelom
Dušan Weiss, Ada Poklač

Tisk
Prograf

Naklada
700 izvodov

Naslov uredništva
Slovensko društvo INFORMATIKA
Uredništvo revije Uporabna informatika
Vožarski pot 12, 1000 Ljubljana
www.drustvo-informatika.si/posta

Revija izhaja četrtletno. Cena posamezne številke je 4.500 SIT. Letna naročnina za podjetja 17.800 SIT, za vsak nadaljnji izvod 11.900 SIT, za posameznike 5.900 SIT, za študente 2.800 SIT.

Revijo sofinancira Ministrstvo za šolstvo, znanost in šport RS.

Revija Uporabna informatika je od številke 4/VII vključena v mednarodno bazo INSPEC.

Revija Uporabna informatika je pod zaporedno številko 666 vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo RS.

Navodila avtorjem

Revija Uporabna informatika objavlja izvirne prispevke domačih in tujih avtorjev na znanstveni, strokovni in informativni ravni. Namenjena je najširši strokovni javnosti, zato je zaželeno, da so tudi znanstveni prispevki napisani čim bolj mogoče poljudno.

Članke objavljamo praviloma v slovenščini, prispevke tujih avtorjev v angleščini.

Prispevki so obojestransko anonimno recenzirani. Vsak članek za rubriko Razprave mora za objavo prejeti dve pozitivni recenziji. O objavi samostojno odloča uredniški odbor.

Prispevki naj bodo lektorirani, v uredništvu opravljamo samo korekturo. Po presoji se bomo posvetovali z avtorjem in članek tudi lektorirali. Prispevki za rubriko Razprave naj imajo dolžino do 40.000, prispevki za rubrike Rešitve, Poročila do 30.000, Obvestila pa do 8.000 znakov.

Naslovu prispevka naj sledi ime in priimek avtorja, ustanova, kjer je zaposlen in elektronski naslov. Članek naj ima v začetku do 10 vrstic dolg izvleček v slovenščini in angleščini, v katerem avtor opiše vsebino prispevka, dosežene rezultate raziskave. Abstract se začne s prevodom naslova v angleščino. Članku dodajte kratek življenjepis avtorja (do 8 vrstic), v katerem poudarite predvsem delovne dosežke.

Pišite v razmaku ene vrstice, brez posebnih ali poudarjenih črk, za ločilom na koncu stavka napravite samo en prazen prostor, ne uporabljajte zamika pri odstavkih.

Revijo tiskamo v črno-beli tehniki s folije, zato barvne slike ali fotografije kot originali niso primerne. Objavljali tudi ne bomo slik zaslonov, razen če niso nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Po možnosti jih pošiljajte posebej, ne v datoteki z besedilom članka. Disketi z besedom priložite izpis na papirju.

Prispevke pošiljajte po elektronski ali navadni pošti na naslov uredništva revije: ui@drustvo-informatika.si, Slovensko društvo INFORMATIKA, Vožarski pot 12, 1000 Ljubljana. Za dodatne informacije se obračajte na tehnično urednico Miro Turk Škraba.

Po odločitvi uredniškega odbora o objavi članka bo avtor prejel pogodbo, s katero bo prenesel vse materialne avtorske pravice na Slovensko društvo INFORMATIKA. Po izidu revije pa bo prejel nakazilo avtorskega honorarja po veljavnem ceniku ali po predlogu odgovornega urednika.

Poslovanje z mislijo na informacijsko varnost

V uredniškem odboru Uporabne informatike smo si nekje na začetku leta zastavili vprašanje, kje smo na področju informacijske varnosti v Sloveniji, in se odločili, da tej temi posvetimo posebno številko. Zavedali smo se pomembnosti tega področja, toda v tej številki objavljeno gradivo potrjuje predvsem to, da smo si pod pojmom informacijska varnost predstavljali različne teme; vdori v računalniške sisteme, protivirusna zaščita, izguba podatkov, varovanje zasebnosti, pooblastila za dostop do podatkov, poslovanje prek spleta, kriptografija in sorodne teme so postale del našega življenja. Drugače niti ne more biti. Živimo v neposrednem stiku z informacijsko tehnologijo. Vse večji del podatkov o nas in našem okolju je shranjen v informacijski obliki. Vse večji del naših življenj se v vsaj enem delu pretoči prek računalnikov. Minili so časi, ko nas je na to, da se nekje v nekem računalniku nahajajo podatki o nas, spominjala le EMŠO. Danes ima podatke o nas shranjene vsak trgovec, ki smo ga vsaj enkrat obiskali, ponudniki kreditnih kartic, društva, katerih člani smo, občinski in državni organi, Zavod za zdravstveno zavarovanje, založniki časopisov in revij, na katere smo naročeni, mobilni operaterji, ponudniki dostopa na internet, podjetja, v katerih smo bili zaposleni, šole, ki smo jih končali, podjetja, s katerimi poslovno sodelujemo. Računalnik shrani naše podatke, ko se z ABC kartico zapeljemo skozi cestninsko postajo na avtocesti, in seveda so naša imena tudi na informacijski avtocesti. Vtipkajte svoje ime v iskalnik Google ali Najdi.si in v nekaj trenutkih bodo pred vami vsi dogodki, vse spletne strani, vse objave v medijih, kjer ste bili omenjeni.

Obstaja tudi druga plat. Brez mobilnega telefona z vsaj nekaj desetimi, če že ne stotimi telefonskimi številkami bi bili čisto izgubljeni. Nobene možnosti nimamo, da bi si jih zapomnili. Podjetja brez podatkov ne bi mogla poslovati. Če ne delujejo računalniške povezave, s kreditno kartico ne moremo plačati niti goriva na bencinski črpalki. Če podjetja ne bi imela shranjenih vseh podatkov o nas, ne bi poznala svojih ciljnih skupin kupcev. Brez informacijske podpore je nemogoče upravljati z viri v podjetju. Podjetje, ki bi ostalo brez vseh svojih podatkov, bi (četudi bi jih imelo vse shranjene v tiskani obliki) potrebovalo več mesecev ali let, da bi vzpostavilo prvotno stanje. Tega časa zagotovo ne bi preživelo. Lahko si le predstavljamo, kaj bi se v primeru večje naravne katastrofe v Sloveniji zgodilo z našimi podatki. Ali bi v času, ko bi ga najbolj potrebovali, deloval naš zdravstveni sistem? Ali bi lahko prišli do denarja v bankah oziroma plačevali z različnimi bančnimi in kreditnimi karticami? Kaj bi se sploh zgodilo s spletom in vse bolj razširjeno elektronsko pošto? Ali je res mogoč najbolj črn scenarij, da vsaj nekaj dni, če že ne tednov ali mesecev, ne bi delovalo nič in bi se tako vrnili v čas pred več kot desetimi leti, ko svet še ni bil e-svet.

Odziv domačih avtorjev na naše povabilo k sodelovanju kaže, da je verjetnost za karkoli podobnega, pa čeprav v manjšem obsegu, majhna. Imamo strokovnjake, ki pokrivajo različna področja informacijske varnosti. To med drugim dokazuje tudi sorazmerno veliko število njihovih prispevkov, od strokovnih do primerov iz prakse in razprav. Če tole številko in vse dogajanje, ki je spremljajo njeno nastajanje, sprejmemo kot pregled trenutnega stanja v Sloveniji, lahko sklenemo, da podjetja, državna ter lokalna uprava informacijski varnosti posvečajo posebno pozornost. Na splošno je poskrbljeno za arhiviranje podatkov ter vsaj osnovno zaščito proti vdorom ter protivirusno zaščito. Prav tako ne poznamo nobenega primera, ko bi podjetje prenehalo poslovati zaradi izgube podatkov ali pa bi zaradi vdora v informacijski sistem zabeležilo večjo poslovno škodo. Večje stroške smo doslej imeli le z odpravo posledic, ki so jih povzročili računalniški virusi.

Ne moremo sicer trditi, da smo na naravne nesreče popolnoma pripravljeni, vendar obstajajo scenariji za delovanje v takih primerih; podjetja in organizacije državne uprave pa za zagotavljanje nadomestnih lokacij namenjajo vse več sredstev.

Zavedanje o pomembnosti tega področja in izvajanje spremljajočih aktivnostih samo po sebi ni dovolj za uvedbo standarda informacijske varnosti ISO 17799 v naše poslovanje. V tej številki si lahko preberete, da je treba za celovit pristop k tej problematiki poskrbeti še za vse kaj drugega, ne le za tehnologijo. Informacije se izgubljajo tudi na naših mizah, v koših za odpadke in nekoliko preveč odprtih osebnih pogovorih. Upoštevate lahko torej vse v tej številki objavljenje prispevke in za varovanje ter zaščito porabite ogromna sredstva, pa se ne boste znebili tistega zadnjega, najšibkejšega člena v verigi: drobne človeške nepazljivosti. Tako smo prišli do skupnega imenovalca: naj so naši pogledi na informacijsko varnost še tako različni, potrebujemo ustrezne standardne in primerljive postopke. Pri tem je ISO 17799 vsaj prava pot, če že ne končna rešitev.

Ostane še odgovor na vprašanje, ki se nam je postavilo samo po sebi. Ali imamo kakšno možnost, da na svetovnem trgu nastopimo z lastnimi rešitvami s tega področja? Brez ustrezne industrije ne moremo ponuditi konkurenčnega in zanimivega izdelka, toda zakaj ne bi ponudili kakšne rešitve ali v kriptografiji uporabnega matematičnega algoritma ali formule, saj se radi pohvalimo s svojim znanjem. Čeprav objavljamo tudi prispevek s področja kriptografije, bomo z izvozom našega znanja očitno morali počakati. Kljub novim priložnostim bo Slovenija na področju informacijske tehnologije in rešitev tudi v prihodnje predvsem uvoznica. Zadovoljni smo lahko že s tem, da je pri nas dovolj strokovnjakov, ki spremljajo svetovne trende in razpolagajo z ustreznim znanjem, ki omogoča vpeljavo ustreznih rešitev v naše okolje. Teža odločitev tako ostaja na strani investitorjev. Toda to je že druga zgodba.

Aljoša Domijan,
gostujoči urednik

Bralcem in sodelavcem

revije Uporabna informatika želimo

srečno in uspešno novo leto 2004

Uredništvo

Učinkovitost kriptografskih funkcij v spletnih aplikacijah

Jasmin Malkić (jasmin.malkic@uni-mb.si)
Tatjana Welzer (welzer@uni-mb.si)
Boštjan Brumen (bostjan.brumen@uni-mb.si)
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Inštitut za informatiko

Povzetek

Skladno z rastjo interneta se povečuje ponudba kriptografskih procedur. Kljub temu so vse procedure in aplikacije zasnovane na določenem številu kriptograpfskih konceptov in operacij.
Članek temelji na ocenjevanju časovne učinkovitosti nekaterih osnovnih kriptografskih operacij pri implementaciji v programskem jeziku Java. Merjenje učinkovitosti vključuje analizo dolžine ključa in generiranje digitalnega podpisa v simuliranju internetnega okolja. Pridobljene rezultate lahko uporabimo za izboljšanje časovne učinkovitosti spletnih aplikacij za varnen prenos podatkov.

Abstract

Performance of Cryptographic Functions in the Internet Applications

The choice of cryptographic procedures applicable on the Internet increases together with the Internet itself. However, all these procedures and applications are based on a few cryptographic concepts and known operations.
The present paper deals with the evaluation of some basic cryptographic operations by means of measuring time performance of their implementation in the Java programming language. The measuring of performance includes analyses of key length and generating of digital signature in the simulation of Internet working environment. The values obtained can be used for improving time performance of Internet systems for secure data transfer.

1 Uvod

Tradicionalna kriptografija na podlagi simetričnega ključa omogoča hitro in zanesljivo enkripcijo. Ker uporablja isti ključ pri enkripciji in dekripciji, se pojavlja problem varne izmenjave ključa. Problem je še posebno očiten, ko govorimo o javnih porazdeljenih računalniških sistemih, kot je internet, kjer se izmenjava izvaja po nezavarovanem komunikacijskem kanalu. Glede na to, da je tajnost ključa bistvena pri zagotavljanju zasebnosti takšne komunikacije, pravimo takšnemu konceptu kriptografija tajnega ključa [5].

V zgodnjih 70. letih sta Diffie in Hellman razvila drugačen koncept s parom ključev za enkripcijo in dekripcijo. Tisto, kar se je začelo kot algoritem za varno izmenjavo tajnega ključa (ki se še vedno pogosto uporablja), je na koncu dalo matematično osnovo za popolnoma nov kriptografski koncept, v katerem se digitalni zapis, kodiran z enim, dekodira le z drugim ključem iz istega para ključev.

V tem primeru se lahko ključ objavi v javnosti in se imenuje javni ključ. Sporočilo, kodirano z uporabo javnega ključa, je lahko dekodirano le z drugim ključem iz para, ki se imenuje privatni ključ, in ga hrani lastnik. Ena od matematičnih osnov za kriptografijo javnega ključa je problem faktorizacije velikega celega števila za iskanje vseh praštevil, ki ga enakomerno delijo. To ni edini primer uporabe kriptografije javnega ključa. Včasih ne potrebujemo enkripcije sporočila, temveč zagotovitev njegovega izvora. Ta problem rešuje koncept kriptografije javnega ključa, imenovan digitalni podpis (angl. digital signature). Če pri podpisovanju sporočila uporabimo tajni ključ, ga lahko preverimo le s primernim javnim ključem. Tako kodirano besedilo je digitalni podpis sporočila in je navadno pri prenosu združeno z izvirnim sporočilom, tako da lahko naslovnik preveri podpis s primerjavo izvirnega sporočila z dekodiranim podpisom pošiljatelja. To je zgolj osnovna zamisel. Dejansko je treba namesto podpisovanja celotnega sporočila podpisati samo njegov MD5 (angl. Message Digest 5) oz. SHA-1 (angl. Secure Hash Algorithm 1) izvleček. Algoritmi za digitalni podpis in njihove procedure generiranja para ključev so podrobno opisani v uradnem poročilu "Digital Signature Standard- FIPS PUB 186-2".

Najbolj pogost algoritem za to vrsto enkripcije je DSA (angl. Digital Signature Algorithm), ki je skupaj

z RSA (angl. Rivest-Shamir-Adleman) in ECDSA (angl. Rivest-Shamir-Adleman) priporočen kot državni standard za digitalne podpise ZDA [8].

Če upoštevamo vse navedeno, ni težko predvideti, da bodo dodatni kriptografski postopki še upočasnili prenos podatkov po omrežju. Pri snovanju varnega internetnega sistema, ki uporablja kriptografijo, je bistvenega pomena izbor prave kriptografske metode in orodij, ki bodo časovno učinkovita. Operacije kriptografije ključa, ki jih mora internetni varnostni sistem opraviti v ustreznem času (in jih je treba analizirati), so:

- generiranje tajnega ključa,
- simetrična ekripcija velikih datotek in sporočil,
- asimetrična enkripcija tajnega ključa,
- digitalno podpisovanje sporočila ali njegovega izvlečka.

Algoritmi za kriptografijo javnega ključa veljajo za bolj počasne v primerjavi z algoritmi, ki uporabljajo tajni ključ. Zato je treba analizirati dolžino kriptografskih ključev za kriptografijo javnega ključa in generiranje digitalnega podpisa. Prva meritev za izboljšanje učinkovitosti kriptografije javnega ključa je večinoma zagotovitev enkripcije manjše količine podatkov. Istočasno je treba zagotoviti, da varnost celotnega sistema ni ogrožena. Prav to je doseženo s podpisovanjem izvlečka sporočila (npr. 20 bytov pri SHA algoritmu) celotnega besedila. Krajši javni ključi pomenijo hitrejšo enkripcijo, ki je primerna za zelo obremenjene pošiljatelje vendar pa predstavlja tveganje za varnost sistema.

Takšne analize se lahko pridobijo le na podlagi točno določene programske implementacije kriptografskega protokola. Sam program je implementiran v objektno orientiranem programskem jeziku Java, ki ima nujno potrebno infrastrukturo ne le za kriptografijo znotraj svojih mrežnih aplikacij, temveč tudi za merjenje učinkovitosti v različnih računalniških okoljih.

2 Standardna in alternativna kriptografija v Javi

Pred pojavom javanskega standardnega razvojnega okolja (JSDK) 1.4.0 so bili javanski kriptografski razredi razdeljeni na "standardne" in "razširitvene". Standardni razredi, imenovani kot dobavitelj storitev kriptografije SUN (angl. cryptography provider), so vključevali podporo za izvleček sporočila, MAC (angl. Message Authentication Code), digitalne podpise DSA in certifikate formata X.509.

Preostanek kriptografskih razredov je bil zapakiran v javansko kriptografsko razširitev (angl. Java Cryptography Extension, JCE) SUN, ki je vsebovala šifrirno orodje za kriptografijo tajnega ključa (angl. symmetric cipher), protokol za izmenjavo tajnih ključev in nekatere posebne implementacije za MAC. Obstajalo je nekaj razlogov za delitev kriptografskih funkcij, med katerimi so posebne izvozne omejitve v ZDA in pogoji za uporabo kriptografije javnega in tajnega ključa (zato JSDK ni bil zmožen enkipcije sporočila).

JCE je pokrival funkcije kriptografije tajnega ključa, posebna implementacija orodja za kriptografijo javnega ključa je bila vključena v drugo javansko kriptografsko razširitev SSL (angl. Java SSL Extension, JSSE), ki je bila namenjena za razvijanje sistema, ki implementira SSL (angl. Secure Socket Layer). Problem z uporabo množičnih razširitev skupaj s standardnimi paketi je bil potreba za dodatno integracijo razširitvenih paketov v sestavljena javanska strežniška okolja (npr. javanski aplikacijski strežniki za servlete).

JSDK 1.4.0, ki je bil dokončan februarja 2002, je prinesel popolno kriptografsko funkcionalnost znotraj svojih standardnih paketov. To dejstvo lahko prihrani čas za konfiguracijo razširitev in ponudi učinkovitejšo kriptografijo z uporabo dodatnih datotek, ki vsebujejo posebno politiko pristojnosti ter dovoljuje dolžine ključev AES (angl. Advanced Encryption Standard) in RSA 128 in 2048 bitov (če to dovoljujejo lokalne oblasti).

Implementacija alternativnega dobavitelja javanske kriptografije praviloma pomeni prepisovanje originalnih SUN javanskih razredov. Zaradi tega so alternativni JCE paketi navadno pisani za posebne namene, ko aplikacija potrebuje algoritem, ki ga SUN ni implementiral ali ga je implementiral na način, ki ne ustreza potrebam.

Da bi bil alternativni JCE operativen, morajo biti arhivske datoteke, ki vsebujejo njegove razrede, vpisane v lokalni sistemski spremenljivki „classpath". Naslednji korak je postavljanje dovoljenj in vpis novega dobavitelja kriptografije v lokalnih javanskih varnostnih mehanizmih in pristojnih datotekah. Da bi delovali v okviru varnostnega sistema, morajo biti novi razredi vpisani poleg ustreznih dovoljenj. Sam dobavitelj kriptografije je lahko vpisan statično v varnostni datoteki (ki lahko vsebuje nekaj dobaviteljev kriptografije) ali dinamično v programu, ki ga uporablja. Klicanje metode za vpis dobavitelja iz programa zahteva manj administrativnega dela, vendar je ta vpis veljaven samo v tem programu.

Nekaj organizacij in podjetij ponuja implementacije alternativnih JCE za izobraževalne namene ali

komercialno uporabo, npr. IBM [3], RSA Laboratories [11], IAIK (TU, Graz) [9], Bouncy Castle Group [10] itn. Te imajo navadno poudarek na izboljšavi izbire kriptografskih algoritmov za objekte tipa Cipher ali Key, kar prizadene te razrede v izvirni implementaciji. Podjetje SUN pomaga pri vključevanju abstraktnih razredov vmesnika za dobavitelje servisov (angl. Service Provider Interface, SPI) za glavne kriptografske objekte, kot so npr. CipherSpi, KeyGeneratorSpi itn. v javansko standardno razvojno okolje. Tisti, ki želijo razviti alternativne dobavitelje kriptografije, lahko implementirajo vse abstraktne razrede in metode, ki so v SPI.

3 Aplikacija za merjenje učinkovitosti javanskih kriptografskih funkcij

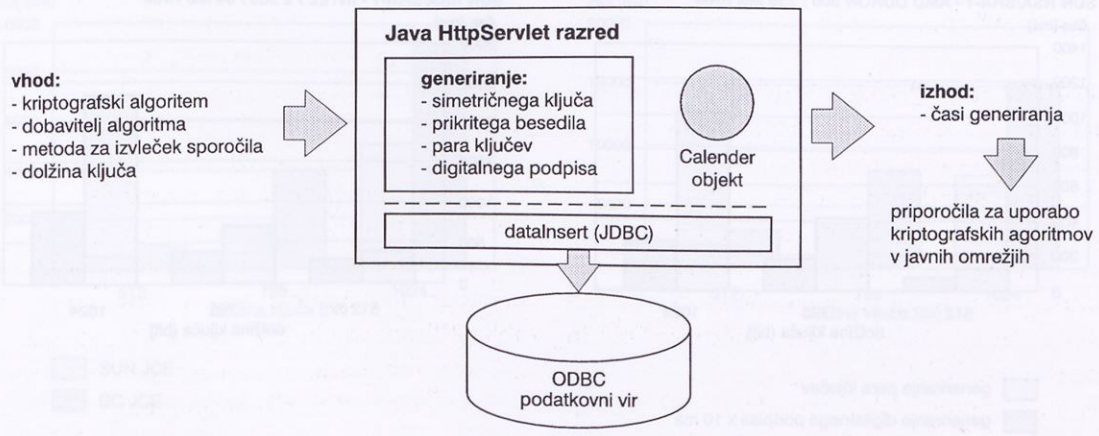
Da bi izmerili učinkovitost izvajanja programskih funkcij na določenem operacijskem sistemu, moramo pravilno uporabiti sistemsko uro. Podpora za časovne objekte (manipulirajo sistemsko uro) v programskom jeziku Java je podana v nekaj razredih, kot sta npr. Date in Calendar. Ker zaradi zastarelosti ne priporočamo uporabe razreda Datum, uporabljamo pri tem testu object tipa Calendar, ki zabeleži lokalni čas točno ob svojemu nastanku. Aplikacija za merjenje učinkovitosti Java kriptografskih funkcij kreira skupno tri primerke objekta Calendar, med katerimi se izvedejo kriptografske operacije, ki jih merimo.

V tem primeru prva vrednost zabeleži nastanek para ključev za algoritem javne kriptografije. Kot vstopne parametre aplikacija vzame algoritem in dobavitelja, za katera se ustvarijo ključi. Druga časovna vrednost vsebuje čas za vpeljavo objekta tipa Signature in proces digitalnega podpisovanja (metoda za izvleček sporočila, ki ga podpisujemo, je vključena v vhodne parametre). Pomemben vhodni parameter za aplikacijo je tudi dolžina ključa. Analiza za algoritem javnega ključa je bila izvedena za dolžine 512, 768 in 1024 bitov. Ta razprava lahko da pregled javanske kriptografije, ki je trenutno v uporabi. Kriptografski ključi dolžine 2048 bitov so dovoljeni samo v najnovejših različicah javanskih delovnih okolij pod posebnimi pogoji (ta uporaba vključuje posebne datoteke za konfiguracijo javanske kriptografske razširitve).

Testna aplikacija razširja HttpServlet razred, ki ga kličemo z http zahtevo (ta vsebuje vhodne parametre) na lokalnem aplikacijskem strežniku za javanske servlete. Njen cilj je meritev učinkovitost v realnemu času in pogojih dinamičnega spletnega okolja. Izid javanskega servleta (slika 1) v http obliki je usmerjen v spletni brskalnik, iz katerega je prišla http zahteva. Rezultati merjenja učinkovitosti se beležijo v lokalni bazi za nadaljnjo analizo. Operacija je izvedena s klicem metode dataInsert, ki lahko izvede vsako poizvedbo na lokalnem ODBC (angl. Open Database Connection) viru podatkov. Izvirna koda metode in celotne testne aplikacije se nahaja na spletnem naslovu http://www.inet.ba/malkic/ird2.

4 Učinkovitost in varnostna analiza

Načrtovanje varnostnega sistema, ki uporablja javansko kriptografijo, zahteva natančno poznavanje kriptografskih orodij, ki naj bi se uporabljala. Za pravilno izbiro kriptografskih algoritmov in dolžino ključev so zaželeni tudi natančni podatki o zmogljivosti posameznih implementacij kriptografskih orodij. Da bi



Slika 1: **Vhodi in izidi testne aplikacije**

dobili takšne podatke, smo izvedli test z zgoraj opisano javansko spletno aplikacijo.

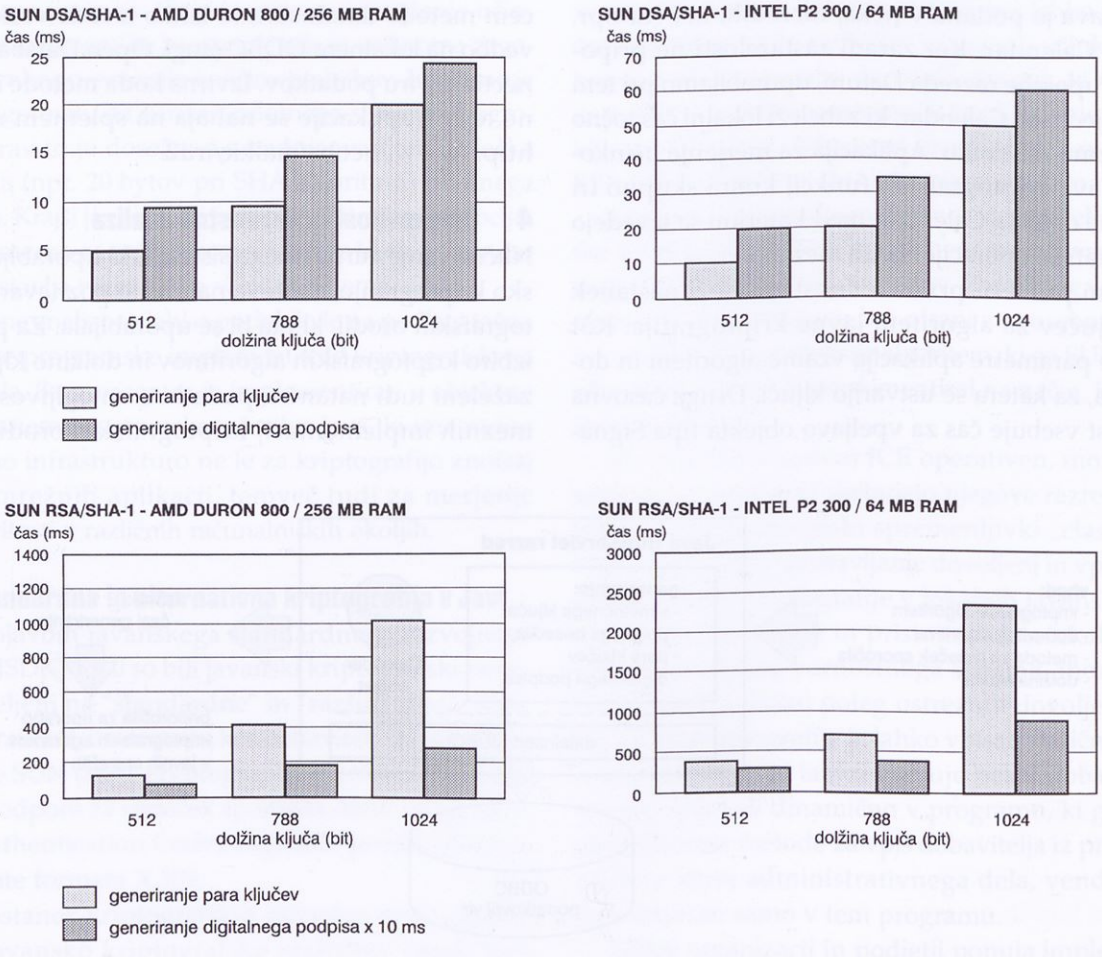
Različni algoritmi za digitalni podpis so podvrženi testiranju/merjenju najpomembnejših karakteristik:

- časa, potrebnega za generiranje para ključev za algoritem kriptografije javnega ključa in
- časa, potrebnega za proces izdelave digitalnega podpisa tekstovne datoteke skupne dolžine 12.650 bajtov na lokalnem trdem disku. V tem delu eksperimenta sta vključena DSA in RSA algoritma iz SUN javanske kriptografske razširitve z uporabo SHA-1 izvlečka sporočila za digitalni podpis.

V primeru enostavnega avtentikacijskega namena ni mogoče pričakovati generiranja para ključev (sistem z več kompleksnosti lahko potrebuje takšno funkcijo). Čas, potreben za operacijo digitalnega podpisovanja, je lahko zelo pomemben pri načrtovanju spletnega kriptografskega sisitema v realnem času. Merjenje je torej narejeno za tri dobavitelje javanskih kriptografskih razširitev – standardni SUN in dve alternativni, IAIK in Bouncy Castle. Omeniti je treba, da je za SUN in Bouncy Castle implementacijo Diffie-Hellmanovega algoritma za ujemanje ključev merjen samo čas generiranja para ključev.

Žal je uporaba nekaterih razširitev tega tipa omejena z njihovimi komercialnimi licencami. IAIK, ki ga je razvil "Institute for Applied Information Processing and Communications, Graz University of Technology", se lahko uporablja za potrebe izobraževanja [9], medtem ko je Boncy Castle kriptografski paket v prosti uporabi [10].

Testiranje na aplikacijskemu strežniku Apache Tomcat 4.1 z dvema kombinacijama strojne opreme naj bi pokazalo, da je relacija med dolžino kriptografskega ključa in časom, potrebnim za operacijo digitalnega podpisovanja z uporabo tega ključa, neodvisna od izbire strojne opreme. Iz slik 2 in 3, je razvidno, da počasnejša strojna oprema potrebuje bistveno več

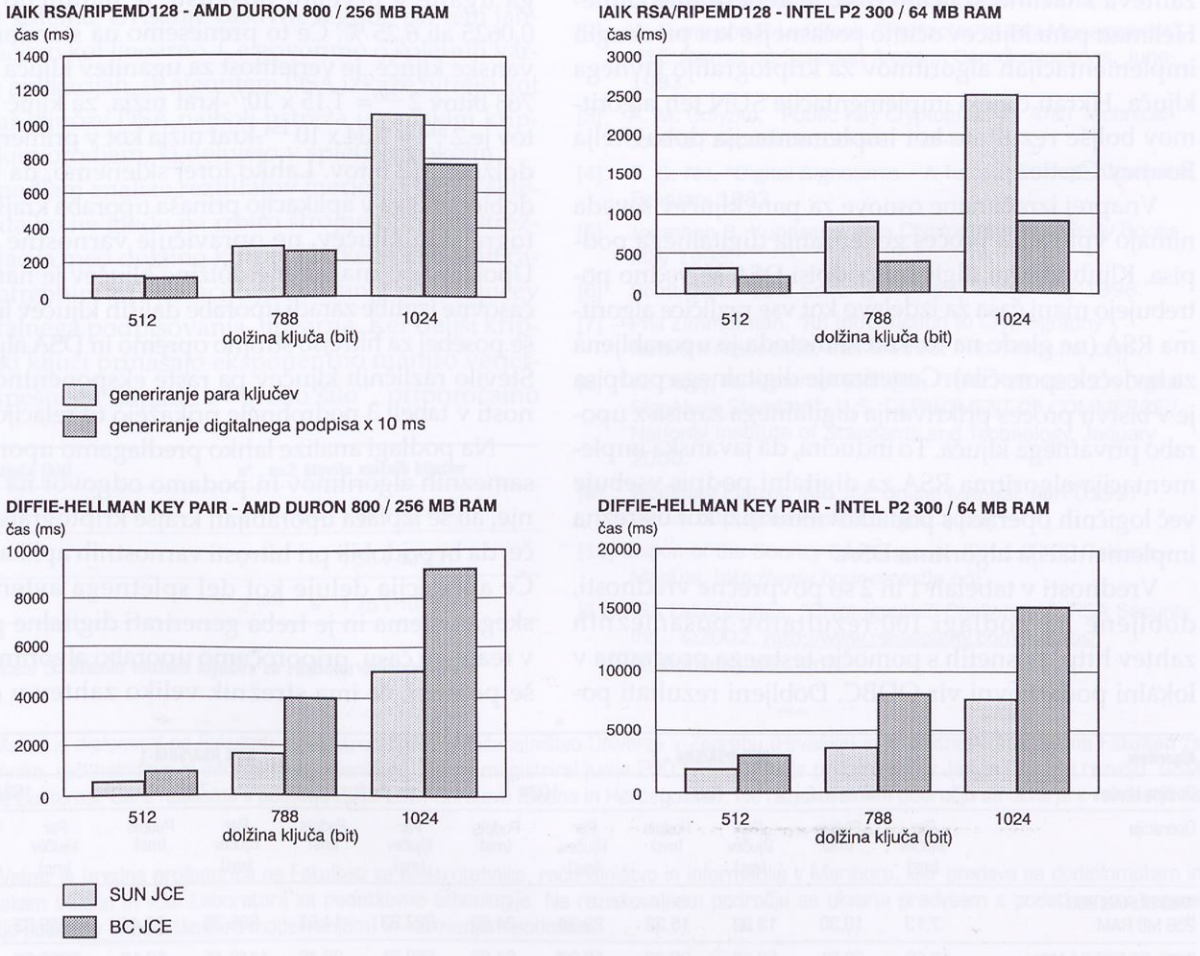


Slika 2: **Vrednosti časa za kriptografske operacije SUN algoritmov za kriptografijo javnega ključa**

časa za izvajanje kriptografskih operacij. Celo iz takšne grobe predstavitve rezultatov lahko sklepamo, da strojna oprema nima značilnega vpliva na trend povečanja časa, ki ga potrebuje proces generiranja para ključev, s povečevanjem dolžine ključa. Izvajanje procesa digitalnega podpisovanja je lahko namreč bolj odvisno od izbire strojne opreme, ker mora testni program v tem primeru napolniti objekt tipa Signature do dolžine 12.650 bajtov podatkov s trdega diska. Program izvede ta proces v 12 delih dolžine 1024 bitov in enemu delu dolžine 362 bitov. Spremenljivi čas dostopa do trdega diska lahko povzroči dodatne časovne izgube, vendar nam merjenje v takšnih pogojih lahko da pregled lastnosti procesa digitalnega podpisovanja. Natančni rezultati merjenja v tabelah 1 in 2 predstavljajo podlago za končno sklepanje.

Izbira algoritma za izvleček sporočila vpliva tudi na izdelavo digitalnega podpisa, saj ima krajši izvleček sporočila (128 bit RIPEMD, angl. RIPE Message Digest) boljši učinek od daljših (kot npr. 20 byte SHA-1). Da bi ta razlika vplivala na rezultate, je treba opazovati samo digitalni podpis izvlečka sporočila. V tem primeru mora biti operacija pridobivanja izvlečka sporočila narejena zunaj programskega bloka, na katerega vpliva merjenje.

Testna aplikacija z uporabo RSA para ključev v Java kriptografskih aplikacijah potrebuje za generiranje para ključev stokrat več časa kot uporaba DSA algoritma. Po drugi strani pa proces generiranja digitalnega podpisa povprečno vzame "samo" dvakrat več časa (zaradi lažje primerjave, so vrednosti za generiranje RSA digitalnega podpisa pomnožene z 10). Do tako velike razlike prihaja zaradi specifične javanske implementacije kriptografskih algoritmov. Za SUN dobavitelja kriptografije in DSA par ključev 512, 768 in 1024 bitov, ima razred KeyPairGenerator na voljo



Slika 3: **Čas, potreben za generiranje para ključev in digitalnega podpisa, za IAIK RSA in D-H algoritme ujemanja ključev**

že izračunan velik sklop primarnih celoštevilčnih vrednosti (ki so osnova za izračun parov kriptografskih ključev). Z uporabo sistemskega naključja in omenjene osnove, KeyPairGenerator lahko dela veliko hitreje kot v primeru drugih algoritmov, kjer se mora material za par ključev generirati v realnem času.

Načrtovalci alternativnega dobavitelja kriptografije lahko integrirajo vnaprej izračunano osnovo v svoje javanske kriptografske razširitvene pakete (JCE) s ciljem, da omogočijo hitrejše izvajanje tudi nekaterim drugim kriptografskim algoritmom. V primeru da zunanji faktorji (kot so zakonske omejitve) preprečujejo uporabo določene implementacije kriptografskega algoritma, se lahko programerske skupine, ki razvijajo varnostne aplikacije, odločijo tudi za razvoj lastnega kriptografskega razširitvenega paketa. Osnova za par ključev algoritma Diffie-Hellman mora tudi biti izračunana v realnemu času iz sistemskega generatorja naključnih števil in dveh velikih praštevil. Ker izdelava te osnove zahteva značilno količino časa, je generiranje Diffie-Hellman para ključev očitno počasnejše kot pri drugih implementacijah algoritmov za kriptografijo javnega ključa. Hkrati dajejo implementacije SUN teh algoritmov boljše rezultate kot implementacija dobavitelja Bouncy Castle.

Vnaprej izračunane osnove za pare ključev seveda nimajo vpliva na proces generiranja digitalnega podpisa. Kljub vsemu digitalni podpisi DSA še vedno potrebujejo manj časa za izdelavo kot vse različice algoritma RSA (ne glede na to, katera metoda je uporabljena za izvleček sporočila). Generiranje digitalnega podpisa je v bistvu proces prikrivanja digitalnega zapisa z uporabo privatnega ključa. To inducira, da javanska implementacija algoritma RSA za digitalni podpis vsebuje več logičnih operacij s podatkovnimi nizi kot ustrezna implementacija algoritma DSA.

Vrednosti v tabelah 1 in 2 so povprečne vrednosti, dobljene na podlagi 100 rezultatov posameznih zahtev http, posnetih s pomočjo testnega programa v lokalni podatkovni vir ODBC. Dobljeni rezultati potrjujejo ugotovitev, da sta celo z različno strojno opremo, časa generiranja para ključev in digitalnega podpisa odvisna od dolžine uporabljenega kriptografskega ključa. Vpliv strojne opreme je omejen na situacije, ko strojna oprema povzroči naključno prekinitev v pretoku podatkov (npr. v primeru generiranja digitalnega podpisa zaradi počasnega dotoka podatkov s trdega diska ali primanjkljaj procesnega časa, ki ga je povzročil "context switch"). Temu se lahko izognemo s hitrejšo in močnejšo strojno opremo ali s ponovljenim merjenjem na slabši opremi.

Glede na varnostne zahteve je treba omeniti, da ima vsak bit v ključu dve možni vrednosti; ključ ima x bitov, zato je število možnih različnih ključev 2^x. Večje število možnih ključev pomeni manjšo verjetnost za uganitev ključa, kar je osnovna operacija napada z grobo silo, pri kateri skušamo preveriti vsak možni ključ. Če je ključ npr. dolg 4 bite, bi ga tak program uganil po vsaj $2^4 = 16$ poskusih. Verjetnost, da ga ugane v prvemu poskusu, je natančno 1/16 = 0,0625 ali 6,25 %. Če to prenesemo na standardne javanske ključe, je verjetnost za uganitev ključa dolžine 768 bitov $2^{256} = 1{,}15 \times 10^{77}$-krat nižja, za ključ 1024 bitov je $2^{512} = 1{,}34 \times 10^{154}$-krat nižja kot v primeru ključa dolžine 512 bitov. Lahko torej sklenemo, da časovni dobiček, ki ga v aplikacijo prinaša uporaba krajših kriptografskih ključev, ne opravičuje varnostne izgube. Upoštevajoč analizirane dolžine ključev je naraščanje časovne izgube zaradi uporabe daljših ključev linearno, še posebej za hitrejšo strojno opremo in DSA algoritem. Število različnih ključev pa raste eksponentno. Vrednosti v tabeli 3 podrobneje prikažejo to relacijo.

Na podlagi analize lahko predlagamo uporabo posameznih algoritmov in podamo odgovor na vprašanje, ali se izplača uporabljati krajše kriptografske ključe, da bi pridobili pri hitrosti varnostnih aplikacij Java. Če aplikacija deluje kot del spletnega avtentikacijskega sistema in je treba generirati digitalne podpise v realnem času, priporočamo uporabo algoritma DSA, še posebej, če ima strežnik veliko zahtev v časovni

Algoritem	**SUN DSA/SHA - 1**						**SUN RSA/SHM-1**					
Dolžina ključa	512		768		1024		512		768		1024	
Operacija	Par ključev (ms)	Podpis (ms)	Par ključev (ms)	Podpis (ms)	Par ključev (ms)	Podpis (ms)	Par ključev (ms)	Podpis (ms)	Par ključev (ms)	Podpis (ms)	Par ključev (ms)	Podpis (ms)
AMD DURAN 900 256 MB RAM	7,13	10,30	13,92	15,32	23,34	24,83	227,83	14,61	685,38	23,44	1258,03	36,63
INTEL P2 300 64 MB	17,63	23,21	33,53	39,89	59,36	64,02	569,81	26,46	1446,45	50,19	2809,69	102,68

Tabela 1: **Povprečna vrednost časa, potrebnega za generiranje para ključev in digitalnega podpisa za SUN algoritme**

Algoritem	IAIK RSA/RIPEMD 128						Diffie-Hellman KA					
Dolžina ključa	512		768		1024		512		768		1024	
Operacija/JCE dobavitelj (ms)	Par ključev	Podpis	Par ključev	Podpis	Par ključev	Podpis	Sun	Bouncy Castle	Sun	Bouncy Castle	Sun	Bouncy Castle
AMD DURON 900 256 MB RAM	232,75	16,20	579,99	34,60	1238,79	62,55	862,18	1145,03	3665,36	4533,28	6795,70	9669,20
INTEL P2 300 64 MB RAM	576,25	23,25	1480,99	51,12	2865,05	104,02	2020,26	3160,25	6204,66	9281,61	11700,57	16526,55

Tabela 2: **Povprečna vrednost časa, potrebnega za generiranje para ključev in digitalnega podpisa za IAIK RSA in D-H algoritme ujemanja ključev**

enoti. Digitalni podpisi DSA potrebujejo manj časa za generiranje ne glede na strojno opremo. Seveda je v primeru manjših količin podatkov (kot so 128-bitni tajni ključi), priporočljiva tudi uporaba algoritma RSA.

5 Sklep

Ker se moč procesiranja sodobnih računalnikov hitro povečuje, je smiselno zvišati varnost sistema z uporabo najdaljšega možnega ključa. Tako se verjetnost za njegovo uganitev eksponentno zmanjšuje, kar zvišuje varnost sistema. Zvišanje časovne izgube pri tem lahko označimo kot linearno. Če govorimo o spletnih varnostnih aplikacijah, se algoritem DSA izkaže hitrejši kot RSA. Par ključev DSA najbolj ustreza javanskim kriptografskim orodjem, ki delujejo v spletnem okolju.

Na podlagi analize rezultatov merjenja lahko sklepamo, da bo ne glede na izbiro strojne opreme strežnika relacija med dolžino kritpografskega ključa in časom, potrebnim za operacijo generiranja para ključev ali digitalnega podpisovanja, linearna. Ker daljši kriptografski ključi prinašajo eksponentno manjšo verjetnost uspešnega napada z "grobo silo", priporočamo njihovo uporabo. Če govorimo o digitalnih podpisih v programskemu jeziku Java, je zaželena uporaba kriptografskega algoritma DSA. Izkazalo se je tudi, da potrebuje proces generiranja para ključev za algoritem Diffie-Hellman ujemanja ključev bistveno več časa, kot druge javanske implementacije algoritmov za kriptografijo javnega ključa.

x, dolžina ključa (bit)	n^x, n=2 število možnih ključev
512	2^{512} = 1,34 x 10 124
768	2^{768} = 1,55 x 10 231
1024	2^{1024} = 1,75 x 10 308

Tabela 3: **Število možnih ključev za različne dolžine ključa**

Viri

[1] M. E. Hellman, "The Mathematics of Public-Key Cryptography", Scientific American, August 1979.

[2] W. Fumy and P. Landrock, "Principles of Key Management", IEEE Journal on Selected Areas in Communications, June 1993.

[3] A. M. Odlyzko, "Public Key Cryptography", AT&T Technical Journal, September/October 1994.

[4] S. G. Akl, "Digital Signatures – A Tutorial Survey", Computer, February 1983.

[5] Jonathan B. Kundsen, "Java Cryptography", O'Reilly Books May 1998.

[6] Scott Oaks, "Java Security", O'Reilly Books May 1998.

[7] Phil Zimmerman, "An Introduction to Cryptography", Network Associates, Inc. ©1998, http://www.nai.com

[8] W. Daley, R. Krammer (Editors), "FIPS PUB 186-2 – Digital Signature Standard", U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology, January 2000.

[9] Wolfgang Platzer, IAIK JCE Online Manual, IAIK Ó1997-2003, http://jcewww.iaik.tu-graz.ac.at

[10] Legion of the Bouncy Castle group, JDK 1.3 JCE Release Manual, http://www.bouncycastle.org

[11] RSA Laboratories, "Cryptographic Challenges", RSA Security Inc., ©2002, http://www.rsasecurity.com/rsalabs/challenges/index.html

Jasmin Malkić je diplomiral na Fakulteti za elektrotehniko in računalništvo Univerze v Zagrebu (Hrvaška) in je doktorski študent na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je magistriral junija 2003. Sodeloval je pri projektih v Javi in C++ pri razvoju "GSM Billing and Customer Care" sistema v podjetju ZIRA Ltd., Sarajevo (Bosna in Hercegovina). Na raziskovalnem področju se ukvarja z varnostjo na internetu.

Tatjana Welzer je izredna profesorica na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer predava na dodiplomskem in podiplomskem študiju in vodi Laboratorij za podatkovne tehnologije. Na raziskovalnem področju se ukvarja predvsem s podatkovnimi bazami (kakovostjo podatkov in podatkovnim modeliranjem) in varovanjem podatkov.

Boštjan Brumen je doktorski študent na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je zaposlen kot asistent za področje informatike. Na raziskovalnem področju se ukvarja s podatkovnimi bazami, podatkovnim rudarjenjem in varovanjem podatkov.

Do IT Investments Have a Real Business Value?

Aleš Groznik, Andrej Kovačič
University of Ljubljana, Faculty of Economics, Kardeljeva ploščad 17, SI-1000 Ljubljana, Slovenia
ales.groznik@uni-lj.si
Mario Spremić
University of Zagreb, Graduate School of Economics and Business, Trg J. F. Kennedya 6, HR-10000 Zagreb, Croatia
mspremic@efzg.hr

Abstract

The business value of information technology (IT) has been debated for a number of years. While some authors attribute to IT large productivity improvements, substantial value added contribution and impact on business performance, others report that IT has not had any bottom-line impact. Although productivity, value added and business profitability are related, they are ultimately separate questions. Using the results of the survey on business informatics situation of 92 Slovene large organizations and 116 Croatian large organizations several relevant hypotheses have been tested. The results show that IT investments reflect in increased productivity and value added. However, the relation between IT investments and business performance has not been confirmed.

Povzetek

Ali je vlaganje v IT poslovno upravičeno?

Pogosto slišimo, da postaja informatika osnovno gibalo uspešne prenove poslovanja v smeri razvoja izdelkov in storitev, kar organizacijam prinaša večjo dodano vrednost oziroma zagotavlja uspešnost poslovanja. Vpliv investicij v informatiko na poslovanje organizacije je zato pogosto vroča tema različnih analiz z nasprotujočimi si rezultati. Namen prispevka je analizirati vpliv naložb v informatiko na dodano vrednost organizacije in njeno uspešnost, pri čemer mero uspešnosti izražamo z več delnimi merami oziroma kazalci uspešnosti poslovanja. Statistična analiza temelji na izsledkih raziskave stanja poslovne informatike v 92 slovenskih in 116 hrvaških podjetjih in omogoča učinkovito primerjavo z razvitim svetom. Rezultati statistične analize izbranih domnev kažejo, da je višina investicij v informatiko v tesni zvezi z ustvarjeno dodano vrednostjo in produktivnostjo, kar pa ne velja za zvezo med višino investicij v informatiko ter donosnostjo in ekonomičnostjo.

1 Introduction

The business value of information technology (IT) investments has earned considerable interest from both academics and business community in recent years. The key question is whether the tremendous amount of IT capital invested in the last few decades has had any impact on the performance of investing organisations. Businesses continue to invest enormous sums of money in IT presumably expecting a substantial payoff. As suggested by Gartner Group (Gartner Group, 2002) IT is becoming a high-expenditure activity. Organizations in developed countries spend between 5 and 7 percent of sales revenue on IT while the majority of Slovene and Croatian organizations invest less than 2 percent of sales revenue into IT. Despite significant investments in IT, the results of a variety of studies present contradictory evidence whether the expected benefits have materialized (Brynjolfsson, 1993), (Wilson, 1993), (Hitt and Brynjolfsson, 1994), (Kraemer and Dedrick, 1994), (Berndt and Morrison, 1995), (Tam, 1998), (Devaraj and Kohli, 2000). Substantial discrepancies are due to the inconsistency of performance measures and ways the IT impact has been measured. Nevertheless all financial ratios should be issued with care since corporate pressures for control often generate behaviors, which subvert both planning are cases where and organizational philosophies and lead to sub optimization. Equally common, the technologists' views of control tend to be in conflict with the philosophy of the management control system in the organization, so that tension and questioning are typical in this area. Finally, as IT becomes perceived as a strategic resource, traditional control questions get a sharper edge. Indeed, they often indicate an erosion of corporate support for IT despite the external and internal rhetorics about IT being a source of competitive advantage.

2 Empirical Analysis

In order to investigate the real business value of IT the following hypotheses have been articulated:

Hypothesis H1: IT investment is related to business performance ratios of the organisation.

Does IT investment affect business performance? That has been a key question for many years. The roots of this question have at least two major streams. On one hand, IT investment is only one of the investments that are undertaken in an organization. By definition, investments are difficult to measure due to the time lag. Apart from the investment there are also other factors that affect business performance. On the other hand, a variety of measures exist to evaluate business performance. For the purpose of our analysis, the following have been used:

Return on Sales (ROS) - a measure of a company's profitability, equal to a fiscal year's pre-tax income divided by total sales.

Return on Assets (ROA) - a measure of a company's profitability, equal to a fiscal year's earnings divided by its total assets, expressed as a percentage.

Return on Equity (ROE) - a measure of how well a company used reinvested earnings to generate additional earnings, equal to a fiscal year's after-tax income (after preferred stock dividends but before common stock dividends) divided by book value, expressed as a percentage. It is used as a general indication of the company's efficiency; in other words, how much profit it is able to generate given the resources provided by its stockholders.

Hypothesis H2: IT investment is related to productivity.

Productivity has been generally defined as a ratio of measure of output to a measure of some or all of the resources used to produce this output. It is the quantitative relationship between what we produce and the resources we use. Defined in this way, one or a number of input measures can be taken and compared with one or a number of output measures. In case of our analysis, the output measure has been total income of the organization whereas the input measure has been average number of employees.

Hypothesis H3: IT investment is related to value added.

Value added evaluates the efficiency by measuring its inputs against its own outputs. The usual basis is the difference between sales income and the cost of goods and bought-in services, adjusted for the changes in level stocks and work in progress. The added value remaining therefore represents the amount available to cover wages and salaries, interest charges, rents and rates, company tax and depreciation. Any remaining net income is a profit from which dividends are paid, the balance being retained by the business to cover innovation and expansion.

As suggested by Hitt and Brynjolfsson (Hitt and Brynjolfsson, 1994), productivity improvement and business performance are not necessarily correlated. Improvements in productivity not necessarily translate into gains in profit measures that can be reflected through business performance. That is the reason why business performance ratios and productivity are separated. For H1, three commonly used performance ratios are used: Return on Equity (ROE), Return on Asset (ROA) and Return on Sales (ROS). These measures are widely used in literature to evaluate the investment. They have been used in previous IT impact studies (Alpar and Kim, 1990), (Hitt and Brynjolfsson, 1994), (Tam, 1998), (Rosser, 1998) creating the basis for comparison.

The basis for H3 is a fashionable concept around which everything else revolves: The integration of value chain. This refers to value added optimization by three ways in which IT assists the enterprise: supply chain optimisation on the back end, interaction with customers on the front end and the linking up of front-end and back-end processes.

In literature the impact of IT has very often been adopted but rarely empirically tested. In this study, we attempt to fill this gap by empirically examining the impact of IT investments on value added.

In order to statistically investigate the above-mentioned hypotheses, a survey has been carried out to highlight the real situation of business informatics in Slovenia. On the basis of the survey the relationship with business performance indicators has been investigated.

3 The Method

3.1 The research in Slovene organizations

The survey in Slovene companies was performed in March 2002 by the IS researchers of the Faculty of Economics in Ljubljana. The survey was based on a questionnaire. The target population included 350 large Slovene organizations taken from a wide range of

industries, randomly chosen from the Business Register, a register of all organizations in Slovenia. According to Slovene legislation (Zakon o gospodarskih družbah, 1993), an organization classifies as large when it meets at least two of the following criteria: number of employees larger than 250, turnover larger than 800.000.000 SIT (approx. 3.500.000 EUR) and total average assets larger than 400.000.000 SIT (approx. 1.750.000 EUR). Comparing this classification to a similar one in the developed countries, it is obvious that the size of the organization can be very relative. In order to ensure that the responses reflect the organizations' perspective, CEOs and IS executives were interviewed to provide information by answering questions about: organization of the IS departments, the state of IS, the concepts and technologies of data storing as well as strategic IS planning and BPR practices. The structure of surveyed organizations are shown in Table 1.

Although small and medium-sized enterprises dominate in Slovene economy, the analysis has been performed on large organizations, in order to compare the results with similar studies conducted in the past (Bergeron et al., 2001), (Hitt and Brynjolfsson, 1996), (Tam, 1998), (Sethi et al., 1993). A total of 92 useful returns have been obtained, representing the database on the situation of business informatics in Slovenia. Table 1 shows the structure of organizations according to the number of employees and their activities. The activities in the category Miscellaneous are consulting, transport, IT, catering, tourism, health service, government, telecommunications etc. The respondents were reasonably well distributed according to the types of business and number of employees, which can be compared to the distribution of all Slovene large organizations (Slovenia in figures, 2000), (Slovene Corporate Law, 1993). Therefore we can generalize the results of the survey to all large organizations in Slovenia.

	Slovene survey		Slovene large organizations
	Number	Percentage	
Structure by type of business			
Manufacturing	36	39,1%	36.5%
Retail and Wholesale	14	15,2%	12.0%
Finance and Insurance	6	6,5%	3.2%
Miscellaneous	36	39,1%	48.3%
Total	**92**	**100%**	
Structure by total number of employees			
< 100	19	20,7%	14,9%
101 - 250	33	35,9%	39,3%
251 - 1000	25	27,2%	29,0%
> 1000	15	16,3%	16,8%
Total	92	100%	

Table 1: **The structure of Slovene organizations based on business type and the number of employees**

3.2 The research in Croatian organizations

The key objective of the research in Croatian companies was to examine a number of issues in current IS practices on a sample of ž400 Largest' Croatian companies, ranked according to 2001 annual revenues. To address the study objectives, a survey questionnaire was considered to be the most appropriate research method.

The questionnaire was preliminary tested on postgraduate and doctoral students for content validity, comprehensiveness and readability. Once a feedback from preliminary testing had been obtained, the questionnaire was pilot tested on five senior IS executives. The 2002 survey was being performed from March 2002 to April 2002. It was carried out by a market research agency who interviewed IS executives. The interview was important since the respondents could not select the questions and topics by themselves.

The questionnaire was sent to 400 IS executives and CEOs in Croatian companies selected from the Register of the ž400 Largest' Croatian companies, which most likely represent the structure of Croatian economy. In the Register, companies were ranked according to 2001 annual revenues. The questionnaire consisted of four parts: structure and current state of IS, organization of IS department SISP practices, business process innovation issues, and e-business practices.

Moreover, it must be mentioned that by Croatian corporate law a company is classified as large when a total number of employees excides 250 and its annual revenue is over 4 million EUR. About 68% of surveyed Croatian companies were large companies according to 2002 annual revenue and 69% had more than 250 employees. Almost a half of Croatian compa-

nies were large according to both criteria: more than 250 employees and revenue over 4 million EUR.

A similar survey was conducted in 2000. The 2000 survey was performed on the same sample (ž400 Largest' Croatian companies according to 1999 annual revenues) and with exactly the same questionnaire, which formed a solid basis for discussion and analysis of trends.

	Croatian survey	
	Number	**Percentage**
Structure by type of business		
Retail and Wholesale	42	36,2%
Manufacturing	21	18,1%
Finance and Insurance	8	6,9%
Miscellaneous	45	38,9%
Total	**116**	**100%**
Structure by total number of employees		
< 50	4	4,3%
51 - 250	5	5,4%
>250	81	88,1%
No answer	**26**	
Total	**116**	**100%**

Table 2: **The structure of Croatian organizations based on business type and number of employees**

Although they represent less than 1% of total number of registered companies in Croatia, the sampled Croatian companies held 73% of the equity capital in the Croatian economy in 2001, accounted for 65% of total Croatian export balance and employed 37% of total number of workers in Croatia. Therefore, the analysis has been performed preferably on large companies enabling us to compare the results with the Slovene and other similar studies (Bergeron et al., 2001), (Hitt and Brynjolfsson, 1996), (Tam, 1998), (Sethi et al., 1993).

We received 116 responses, which can be considered a strong response rate of 27%. Table 2 shows the structure of the surveyed Croatian companies according conomic activity (based on European Classification of Economic Activities – NACE Rev.1) and total number of employees. More than one-half of the responding companies come from only two industry branches, (wholesale and retail trade - 36.2% and manufacturing - 18%) and that can be considered representative for the overall structure of Croatian economy, with trade as prevailing economic activity as opposed to manufacturing. The activities in the category Miscellaneous referred to various types of business, such as transport, tourism, IT, telecommunications, finance and insurance, real estate, government.

Furthermore, the surveyed companies were evenly distributed through Croatia, though the majority are located in Zagreb, the capital and economic center of Croatia, and in the surrounding areas of Zagreb, so that a regional bias in the results cannot be excluded. Regional issues were less important in the 2001 annual revenues. Regarding the sample, proposed methodology and professionalism in planning and conducting the research, the results may be considered representative for large companies in Croatia.

4 The Results

According to Gartner Group (Gartner Group, 2002) IT is becoming a high-expenditure activity. Gartner's survey results show that companies in developed countries (North America, Western Europe, Asia/Pacific region) spend between 5 and 7 percent of sales revenue on IT. By 2005, Gartner forecasts that investments in e-business applications and infrastructure will drive average IT spending in North America beyond 10 percent of revenue. The situation in Slovene and Croatian companies differs significantly. According to our surveys approximately 60 percent of them invest less than 2 percent of sales revenue into IT. The results also show that by the year 2000 only 5 percent of Slovene companies and by the 2002 also 6 percent of Croatian companies will have invested more than 5 percent of revenue into IT (Table 3). Even thought the number of Slovene and Croatian companies investing significant share of revenue into IT is increasing, the overall lack of investing into IT is still predominant.

The analysis of real business value of IT is based on χ^2 test, testing the relationship between IT investment and selected key indicators. The results are shown in Tables 4-7. Sample sizes differ since not all financial data has been available publicly. As can be noticed from Tables 4-6 there is no data for Croatian study for year 2000.

As shown in Table 4, IT investment does not correlate with business performance. Having in mind 5% significance level, a test between IT investment and ROS shows a weak relationship (χ^2=10,516, p=0,105)

	Slovene companies			Croatian companies		
	0%-2% of the revenue	2%-5% of the revenue	above 5% of the revenue	0%-2% of the revenue	2%-5% of the revenue	above 5% of the revenue
1999	64%	32%	4%			
2000	67%	27%	5%	64%	24%	12%
2001	52%	34%	13%			
2002				61%	33%	6%

Table 3: **IT investments in Slovene and Croatian companies**

but nevertheless the H1 is not supported. This finding is somehow in line with previous studies (Tam, 1998), (Weill, 1992) where no clear indication of relationship between the IT investment and business performance ratios are reported since the results differ from one country to another.

	Slovene study (2000)		
	ROS	ROA	ROE
χ^2	10,516	4,024	3,246
p	0,105	0,673	0,758
Sample Size	82	82	82

Table 4: **The Impact of IT investments on business performance in Slovene study**

	Slovene study (2000)	
	Productivity	Value added
χ^2	9,997	11,266
p	0,040	0,026
Sample Size	92	92

Table 5: **The Impact of IT investments on productivity and value added in Slovene study**

For productivity and value added, the study shows a strong relationship in Slovene 2000 study (χ^2=9,997, p=0,040 for productivity, χ^2=11,266, p=0,026 for value added) thus we can support H2 as well as H3. This finding is also in line with comparable studies (Brynjolfsson, 1993), (Hitt and Brynjolfsson, 1996), (Hoffman, 1997).

Since IT investments have a lag effect, we performed the same analysis as described above for the time lag of one year. For this analysis we used business performance data for Slovene companies for the year 2001 and compared them to the survey findings in 2000.

Also, here we added the results of Croatian 2002 study and compared them to the similar Slovene ones.

The results of performance are very similar to results with no time lag effect. Like the analysis with no lag, there is no relationship of IT investment with ROA and ROE. For ROS results indicate the existence of a lag effect. Also, Croatian study had some difficulties in reaching all required business ratios (only ROS was available for comparison). Nevertheless that in both cases the results of the analysis show a weak relationship, the H1 cannot be supported.

Results for H2 and H3 are identical to those without a lag. For productivity and value added, the Slovene study again shows a strong relationship (χ^2=10,756, p=0,039 for productivity, χ^2=10,489, p=0,043 for value added) thus, in Slovene case we can support H2 as well as H3 even in a case of a time lag.

Croatian study results showed no relationship between IT investments and productivity and value added. Some prior researches (Spremic et. al., 2002) showed that Croatian companies underestimate necessity of IS strategic planning, that CEOs have reactive attitude toward IT initiatives, and that organizational position of IT function is inadequate, with the final conclusion that Croatian companies are just keeping present IS in working conditions on the same level of technology with no initiative for its improvement and development. Therefore, in such a reactive environment, major influence on overall productivity or value added cannot be expected.

5 Discussion and Limitations

In this paper we investigated the impact of IT investment on business performance, productivity and value added. Since the question of the survey has been structured into a pre-set multiple question (IT investment

	Slovene study (2001)			Croatian study (2002)
	ROS	ROA	ROE	ROS
χ^2	11,236	3,269	4,569	2,949
p	0,956	0,596	0,621	0,229
Sample Size	82	82	82	90

Table 6: **The Impact of IT investments on business performance (One year lag)**

	Slovene study (2001)		Croatian study (2001)	
	Productivity	Value added	Productivity	Value added
χ^2	10,756	10,489	4,920	3,062
p	0,039	0,043	0,296	0,547
Sample Size	92	92	90	90

Table 7: **The Impact of IT investments on productivity and value added (One year lag)**

0%-2% of the revenue, 2%-5% of the revenue and above 5% of the revenue) our method slightly differed from previously adopted methodologies. Nevertheless, the results of the study reveal important guidelines.

The current study enables us to compare the results of one economy to other economies and allows cross-national research comparison. This is particularly important since IT investments are the key issue of companies worldwide and the results based on a single economy need to be tested and confirmed across borders to establish external validity.

There are several limitations of the data used in the studies. Ideally, we wanted to incorporate all components that are considered IT investment into our measure. Interviewers were instructed in detail that for the purpose of the survey IT investment consists of broad definition including hardware and software investments, support costs and complementary investments (such as training costs, designing and implementing business processes). Since such a definition of IT investment is generally not easily shown in accounting, detailed data on the totality of IT investments is generally not available. That was the main reason, that we decided to split the answer on IT investment of a particular company into three levels (0%-2% of the revenue, 2%-5% of the revenue and above 5% of the revenue).

Second, the Slovene survey data were self-reported which could lead to errors in reporting and sample selection bias. However, the large size of the sample helped mitigate the impact of data errors. Since the respondents were reasonably well distributed according to the types of business and number of employees we can generalize the results of the survey to the population of large organizations in Slovenia. The Croatian study was carried out by a market research agency by means of interviewing IS executives.

For the purpose of taking into account the time lag effect, the analysis of IT investment on business performance as well as productivity and value added was carried out. Someone might oppose that a one-year lag may not capture all of impacts because companies may not realize all the benefits of IT investments for several years. On the other hand, IT investments have extremely short lifetime and short-run competitive advantage. The short-run competitive advantage such as first mover advantage of new IT applications cannot be sustained for a longer period. We believe that one-year time lag best captures the effect of IT investment.

Our findings suggest that the relationship between IT investment and business performance could be a more complex issue. The findings on ROS, ROA, ROE, when combined with empirical studies conducted in the United States (Sethi et al., 1993), (Weill, 1992) and Asia/Pacific region (Tam, 1998) indicate that the impact of IT investment on business performance might not be a direct one and a variety of other factors that are institutionally and socially related also have an important impact.

On the other hand, numerous organization–level studies and analyses show that IT can contribute substantially to the company's productivity growth. This contribution is by all means strong where IT strategy is linked with business strategy, thus IT can initiate major changes in organization structure, business processes and overall activities. In one study, Brynjolfsson and Hitt (1993) concluded 'that while computers make a positive contribution to productivity growth at the firm level, the greatest benefit of computers appears to be realized when computer investment is coupled with other complementary investments; new strategies, new business processes, and new organizations all appear to be important.' Dvorak et al. (1997) argued about the IT management issues and showed that successful companies manage IT functions in much the same way that they manage their other critical functions and processes: by strong leadership at highest level, by treating IT primarily business activity

and by focusing IT efforts on creating added business value.

According to the 2002 survey result, only a moderate number (48,1%, or 51 out of 106) of Croatian companies linked their IT strategy with business strategy. This linkage is well recognized through process of strategic IS planning. Therefore, almost half of the Croatian largest and strongest companies do have a strategic IS plan, which is in line with the Slovene study result (44,6%, or 41 out of 92). In addition, the linkage between IT strategy and business strategy can also be seen through some organizational issues, namely IT manager's position (low hierarchy level) and organizational position of IS (mainly supportive position).

In case of IT investment, the effect of the IT deployment needs to be addressed. An important factor is the type of IT deployment. IT investment covers all types of IT applications. When innovating, the main goal is to invest as much as possible into innovative systems developing strategic and innovative applications. According to Dos Santos (Dos Santos et al., 1993) the financial market values IT investments selectively. As found in their study shareholders value IT investments that are innovative in nature. By investing into innovative systems shareholders expect gaining comparative advantage resulting in positive impacts on business performance.

Productivity is the fundamental economic measure of a technology's contribution. The lack of good quantitative measures or the output and value created by IT have made MIS manager's job justifying investment particularly difficult. Almost two-third of surveyed Croatian companies (65%) don't have any formal measures or generally accepted metrics to evaluate the impact of their IS on productivity, although they are very much aware of their importance (average mark 3,95 on 1-5 scale for the importance of having or implementing such a measure). Academics have had similar problems assessing the contribution of the new technology and this has been generally interpreted as negative signal of its value. The disappointment in IT has been described in articles disclosing broad negative relationship with IT and productivity (Baily and Chajrabarti, 1988), (Baily and Gordon, 1988), (Berndt and Morrison, 1991), (Franke, 1987), (Loveman, 1988), (Panko, 1991). According to Brynjolfsson (Brynjolfsson, 1993) the productivity paradox of information technology has had several reasons (mismeasurement of outputs and inputs, lags due to learning and adjustment, redistribution and dissipation of profits, mismanagement of IT). After reviewing and assessing the research to date, it appears that the shortfall of IT productivity is due rather to deficiencies in the measurement and methodological tool kit as to mismanagement by developers and users of IT (Brynjolfsson, 1993). The findings of our study are in line with other studies on productivity and IT investments (Brynjolfsson and Hitt, 1996), (Tam, 1998), indicating that IT has increased productivity.

Evaluating investments in information technology poses a number of questions associated with valuing intangible resources, the problem not present when investing in traditional assets. Banker et al. (1993) stressed that, concerning IT investing, focus shifts from measuring hard and quantifiable benefits that will appear on the company's financial reports to measuring indirect, diffuse, qualitative and intangible impacts that are very difficult to measure.

Therefore, to gain a profit from huge IT investments and to make computers effective in use, companies need to make similar investments in software, training, human capital, intellectual capital and organizational changes, which together create intangible assets.

According to the results of the survey, Croatian organizations plan to spend the biggest amount for hardware and the smallest for office software and education of employees. Also, financial situation of the firm greatly influences the level of investments in IT, while industry type, orientation to the foreign markets, type of the ownership and origin of the firm's capital do not have much impact.

The principle of the role of information is best described by value chain analysis. The overall performance of the industry in terms of its ability to maximise value added and minimise its costs is dependent on how well demand-and-supply information is matched at all stages of the industry. To achieve business excellence, the resources of the industry need to be focused on producing goods and offer and perform services as efficiently as possible to the satisfaction of consumers. If poor information means that those resources are wasted or used inefficiently, costs rise without an increase in revenue, and business performance an increase heads down. Understanding the industry value chain, and the key information flows in the industry, a company can intercept and influence

those information flows to its advantage, to the benefit of its trading partners and at the expense of its own competitors. Whilst this ability is not a substitute for good products and services or good marketing, it can complement their strategies and ensure that the company maximizes the profits over the long run. The strong relationship between IT investment and value added can be empirically depicted from results in Table 4 and 6.

6 The Conclusion

The results of our study indicate that Slovene and Croatian companies are increasingly investing into IT. Even though Slovene and Croatian organizations invest significant share of revenue into IT, the overall lack of investing into IT is still predominant. While companies in developed countries (North America, Western Europe, Asia/Pacific region) spend between 5 and 7 percent of sales revenue on IT by the year 2000 only 5 percent of Slovene organizations and 6 percent of Croatian organizations in 2002 invested more than 5 percent of revenue into IT.

But what is the business value of IT? In this paper we investigated the impact of IT investment on business performance, productivity and value added. The results show that IT investments reflect an increased productivity and value added. However, the link between IT investments and business performance has not been confirmed.

7 References

[1] Alpar P. and Kim M.:
A Microeconomic Approach to the Measurement of Information Technology Value. Journal management Information Systems, 7, 2 1990, pp. 55-69.

[2] Baily M., Chajrabarti A.:
Electronics and White-Collar Productivity. Innovation and the Productivity Crisis, Brookings, Washington, 1988.

[3] Baily M., Gordon R. J.:
The Productivity Slowdown, Measurement Issues and the Explosion of Computer Power, Brookings Papers on Economic Activity, The Brookings Institution, Washington, 1988.

[4] Berndt E. R., Morrison C. J.:
High-tech Capital, Economic and Labor Composition in U.S. Manufacturing Industries: An Exploratory Analysis. National Bureau of Economic Research, Washington, 1991.

[5] Berndt E. R., Morrison C. J.:
High-tech Capital, Economic and Labor Composition in U.S. Manufacturing Industries: An Exploratory Analysis. Journal of Econometrics, 65, 1, 1995, pp. 9-43.

[6] Brynjolfsson E.:
The Productivity Paradox of Information Technology. Association for Computing Machinery, Communications of the ACM, New York, 1993.

[7] Brynjolfson, E. and Hitt, L.M.:
Is information systems spending productive? New evidence and new results, Proceedings of the International Conference on Information Systems,Orlando, FL, pp. 47-64., 1993.

[8] Dos Santos B. L., Peffers K., Mauer D.C.:
The Impact of Information Technology Investment Announcements on the Market Value of the Firm. Information Systems Research, 4, 1, 1993, pp. 1-23.

[9] Devaraj S. and Kohli R.:
Information technology Payoff in the Health-Care Industry: A Longitudinal Study. Journal of Management Information Systems, 6, 4, 2000, pp. 41-67.

[10] Dvorak, R.E., Holen, E., Mark, D., Meehan, W.F. :
Six principles of high-performance IT, McKinsey Quartertly, Number 3, 1997, pp. 164 – 177.

[11] Earl M. J.:
Strategies for Information Technology, Prentice Hall International, 1989.

[12] Franke R. H.:
Technological Revolution and Productivity Decline: Computer Introduction in the Financial Industry. Tech. Forecast. Soc. Change, 31, 1987.

[13] Gartner Group:
IT Spending: Its History and Future, www.gartnergroup.com, 23.10.2002.

[14] Groznik, A., Spremić, M.:
Towards a Model of SISP Practices in Transition Countries – Comparative Study of SISP Practices in Slovenia and Croatia, Proceedings of the 6th International Symposium on Operational Research in Slovenia, Preddvor, Slovenija, 2001, pp. 375-380.

[15] Hitt L. and Brynjolfsson E.:
The Three faces of IT Value: Theoryand Evidence. Proceedings of the 15th International Conference on Information Systems, 1994.

[16] Hoffman T.:
Feds Link IT, productivity but hard evidence lacking. Computerworld, 31, 34, 1997.

[17] Kraemer K. and Dedrick J.:
Payoffs from Investment in Information Technology-Lessons from the Asia-Pacific Region. World Development, 22, 12, 1994, pp. 1921-1931.

[18] Loveman G. W.:
An Assessment of the Productivity Impact on Information Technologies. MIT Management in the 1990s working paper 88, 1988.

[19] Panko R. R.:
Is Office Productivity Stagnant? MIS Quaterly, June 1991, pp. 190-203.

[20] Rosser B.:
Making IT Investments Cost Effective. Forbes, 1998, pp. 50-54.

[21] Sethi V., Hwang K. T., Pegels C.:
Information Technology and Organizational Performance. Information & Management, Amsterdam, 25, 1993, pp. 193-205.

[22] Slovenia in Figures '99, Statistical Office of the Republic of Slovenia, 2000, www.sigov.si/zrs

[23] Slovene Corporate Law (Zakon o gospodarskih družbah), Official Gazette RS 30/93, Ljubljana, 1993.

[24] Spremić, M., Strugar, I.:
Strategic IS Planning Practise in Croatia: Organizational and Managerial Challenges, International Journal of Accounting Information Systems, Vol. 3, Num. 3, 2002., pp. 183-200.

[25] Tam K. Y.:
The Impact of Information Technology Investments on Firm Performance and Evaluation: Evidence form Newly Industrialized Economies. Information Systems Research, 9, 1, 1998, pp. 85-98.

[26] Thurow L.:
Economic Paradigms and Slow American productivity Growth. Eastern Eco.J. 13, 1987, pp. 333-343.

[27] Weill P.:
The Relationship Between Investment in Information Technology and Firm Performance. Information Systems Research, 3, 4, 1992, pp. 307 – 333.

[28] Wilson D.:
Assessing the Impact of Information Technology on Organizational Performance. Strategic Information technology Management, Idea Group, 1993.

[29] Zakon o gospodarskih družbah, Official Gazette 30/93, 1993.

▪

Aleš Groznik is assistant professor in the Department of Information Sciences at the Faculty of Economics, University of Ljubljana. He holds a first degree and a M.Sc. in Engineering and a M.Sc. and Ph.D. in Information Sciences from University of Ljubljana. He has extensive industry experience in management and strategic information systems gained working for several multinationals. His research interest is in the areas of information system role within the broader context of corporate objectives, management and strategic information system planning, information technology productivity, information technology management and the role of information systems in ever changing business environments.

▪

Andrej Kovačič is professor at the Faculty of Economics, University of Ljubljana. He was engaged as consultant and project manager on more than 30 Business Process Reengineering (BPR) and Information System (IS) development projects. He is a certified: Expert on Management Consulting and Information Technology, and Information Systems Auditor. He is also Editor of the Slovene review for business informatics Uporabna informatika, and member of Slovene Society of Informatics.

▪

Mario Spremić received a B.Sc. in Mathematical Sciences, M.Sc in IT Management and Ph.D. in Information Systems from the University of Zagreb. He is assistant professor of IT Management and Business Computing at the Graduate School of Economics and Business, University of Zagreb, at the Department of Information Sciences. His current research interests focus on information system strategy, IT management, business process management and e-business models. He has also worked as a programmer, software engineer and project manager.

Časovno žigosanje, nujna sestavina varnega e-poslovanja v javni upravi

Mitja Dečman
Univerza v Ljubljani, Fakulteta za upravo
mitja.decman@fu.uni-lj.si

Marjan Krisper
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
marjan.krisper@fri.uni-lj.si

Povzetek

Uspešno uvajanje elektronskih storitev je eden glavnih ciljev sodobne e-uprave in uspeh uvajanja je v veliki meri odvisen tudi od uporabnikov in njihovega zaupanja v storitve, varno e-poslovanje in zasebnost njihovih osebnih podatkov. Digitalni podpis je varnostni element, ki je pogosto prisoten v takih storitvah, vendar ima nekaj kritičnih pomanjkljivosti, ki jih lahko odpravimo z uporabo časovnega žiga. Časovni žig ne dodaja samo varnega zapisa časa, temveč ponuja mnoge dodatne lastnosti, ki povečujejo stopnjo varnosti in zaupanja med uporabniki. Ker so digitalna potrdila precej razširjena v današnji informacijski družbi za elektronsko identifikacijo ali overjanje, je uvedba in uporaba digitalnih podpisov dokaj preprosta. Vendar mora biti natančno načrtovana, saj imajo pomanjkljivosti, ki peljejo do zlorab, kritične razsežnosti. Brez popolnega zaupanja uporabnikov v e-upravo in njene storitve pa le-te ne bodo nikoli zaživele. Slovenska uprava ima trenutno kljub dobri infrastrukturi in pravnim podlagam zelo malo dobrih in zaupanja vrednih storitev, ki bi vključevale digitalno podpisovanje. Razlog za to je tudi pomanjkljivost digitalnega podpisa.

Abstract

Time stamping, the necessary component of safe e-business

Successful delivery of electronic services is a prime goal of modern e-government and their introduction will be successful only if users that the services, e-government and privacy of their personal data. Digital signature is an enabling security element of these services but it has a few critical deficiencies that can be surpassed with the use of time stamp. It does not only add a precise time to the data but also offers many elements that increase security and trust. Since digital certificate is widely used for authentication, digital signature should be easily implemented. However, the implementation has to be studied carefully as the abuse can have critical dimensions. Without utmost percent trust of users, e-government and its services will never come to life. Slovenian e-government is in at present supported by good infrastructure, good legal background, but has very few trusted services. One of the reasons is deficiency of digital signature.

Uvod

Javna uprava mora slediti modernizaciji družbe in najnovejšim tehnološkim dosežkom. To kažejo tudi koristi, ki so opazne v zasebnem sektorju. S pomočjo informacijske tehnologije je mogoče doseči in zadovoljiti več uporabnikov in povečati kakovost dela. Na eni od nedavnih konferenc na temo e-uprave je bilo podanih nekaj tez glede omenjenega razvoja [12]. Ena od tez govori, da je ponujanje storitev uspešno le, če imajo uporabniki storitev (državljani, zasebni sektor ali zaposleni v upravi) zaupanje pri izvajanju transakcij in zaupajo e-upravi.

Enaka raven zaupanja se je zahtevala v preteklosti in bo zaželena tudi v prihodnje. Za doseganje varnostnih ciljev je treba uporabiti različne tehnike in poiskati celovite rešitve. V primeru zaupanja in varnosti govorimo o overjanju, celovitosti, nezanikanju, zaupnosti in avtorizaciji.

Ena najbolj razširjenih tehnologij za zagotavljanje različnih varnostnih funkcij je infrastruktura javnih ključev (angl. public key infrastructure – PKI), ki temelji na asimetrični kriptografiji in digitalnih potrdilih. Pošiljatelj ob uporabi naslovnikovega javnega ključa in programske opreme, ki pozna šifrirni algoritem, izdela šifrirano sporočilo v elektronski obliki – tajnopis. Nato sporočilo digitalno podpiše z uporabo svojega tajnega ključa. Vse skupaj nato pošlje naslovniku. Postopek torej ostaja enak, le tehnike so se od rimskih časov spremenile in se bodo verjetno spreminjale tudi v prihodnje.

Varne storitve v e-upravi

Pri prehodu v informacijsko družbo se dokumenti namesto na papirju vse pogosteje pojavljajo v elektronski

obliki. Komuniciranje poteka prek računalniških omrežij, interneta in intraneta. Lastnoročni podpis se umika elektronskemu. V procese v zasebnem in javnem sektorju se vključuje nove tehnologije in zaradi tega pogosto uvede nov način dela. V novem okolju je treba zagotoviti varnost in zaupanje za izvajanje teh procesov. Eno od področij, na katero prodira informatizacija, je tudi uprava, ki počasi postaja e-uprava. Ta je torej tisti del celotnega sistema javne uprave, ki uporabniku na podlagi uporabe sodobne informacijske tehnologije ponuja bistvene informacije in storitve kjerkoli, kadarkoli in kakorkoli, na vseh ravneh upravljanja in vodenja ter jo ta uporablja za spremembo načina in vsebine svojega delovanja – za modernizacijo. E-uprava kot nova oblika uprave in upravljanja se vsakodnevno srečuje z novimi izzivi. Večina držav že izvaja različne strategije in akcijske načrte, politiki obljubljajo boljše življenje v novi družbi. Uporabniki ob poslušanju in spoznavanju pričakujejo veliko. Če bodo storitve, ki jih ponuja e-uprava, zadovoljile njihove potrebe, jih bodo tudi uporabljali, sicer bo ves trud zaman. Zatorej je vse odvisno od uporabnikov. Storitve morajo biti učinkovite, hitre, preproste za uporabo in varne. Uporabniki morajo zaupati v tehnike, ki storitve podpirajo. Zato mora e-uprava skrbno preučiti in uporabiti najbolj napredne, a hkrati zanesljive varnostne tehnologije, da si pridobi zaupanje uporabnikov in uspe.

Digitalni podpis, digitalno potrdilo in časovni žig

V elektronskem svetu obstajajo dokumenti[1] v elektronski obliki in tako kot podpisujemo papirne dokumente, potrebujemo podoben postopek za podpisovanje dokumentov v elektronski obliki. Podobno kot lastnoročni mora tudi elektronski podpis dokazovati pristnost in dokončnost dokumenta [11]. Unikatni podpis mora biti tak, da je kasneje mogoče dokazati, da se je podpisal prav ta podpisnik. Elektronski podpis je lahko katerikoli podpis v elektronski obliki, medtem ko je digitalni podpis posebna oblika elektronskega podpisa, izdelana z uporabo asimetrične kriptografije in pripadajočih algoritmov. Asimetrična kriptografija je danes ena najpogosteje uporabljenih metod in temelji na paru različnih ključev (tajni in javni), ki sta matematično povezana[2] [1]. Tajni ključ je niz bitov, ki je varno shranjen pri lastniku, pogosto na pametni kartici ali osebnem računalniku in zaščiten z geslom. Drugi, javni ključ, je na voljo vsakemu uporabniku, vendar je ugotovitev tajnega ključa iz javnega nemogoča oz. neizračunljiva v razumnem času. Tajni ključ je uporabljen za izdelavo podpisa, medtem ko je javni ključ potreben za preverjanje podpisa. Pomembna razlika v primerjavi s simetrično kriptografijo, ki se je pojavila že prej, je, da je pri simetrični kriptografiji za šifriranje in dešifriranje uporabljen enak ključ. Vendar v tem primeru nastane problem izmenjave ključa, torej kako naj pošiljatelj, ki je generiral ključ, le-tega varno dostavi prejemniku, ki mora sporočilo dekodirati. Te težave pri asimetrični kriptografiji ni, saj je ključ za preverjanje podpisa javen in dostopen vsakomur. Uporabnik, ki želi uporabljati digitalni podpis, s pomočjo ustrezne programske ali strojne opreme izračuna par ključev. Tajni ključ varno shrani in zaščiti z geslom, javni ključ pa objavi. Lahko ga tudi pošlje osebam, s katerimi želi varno komunicirati po elektronski pošti.

V procesu podpisovanja podpisnik šifrira dokument s svojim tajnim ključem. V resnici podpisnik v praksi podpiše povzetek dokumenta. Povzetek je nekakšen prstni odtis podpisanega dokumenta in je izdelan s pomočjo zgostitvene funkcije, ki kot rezultat vrne povzetek fiksne dolžine, izračunan iz podatkov poljubne dolžine. Zgostitvena funkcija je natančneje imenovana enosmerna nekolizijska zgostitvena funkcija. Njena bistvena lastnost je, da nihče ne more na podlagi povzetka (v razumnem času) izračunati ali pridobiti podatkov ali rekonstruirati dokumenta. Prav tako je (v razumnem času[3]) nemogoče izdelati dva različna dokumenta, ki bi kot rezultat zgostitvene funkcije dala enak povzetek. Prednost uporabe kratkega povzetka pri digitalnem podpisovanju je hitrejši izračun podpisa in njegova manjša dolžina. Torej je tehnično gledano digitalni podpis niz bitov, pridobljenih s kodiranjem povzetka s pomočjo tajnega ključa podpisnika, kjer je povzetek enolična predstavitev podpisanega dokumenta.

---

[1] *Dokument – informacijski objekt, ki je predstavitev kakršnihkoli podatkov, kot je besedilo, fotografija, video ali zvočni zapis, računalniški program ali kakršnakoli druga oblika podatkov oz. kombinacija le-teh, urejenih ali neurejenih, podana na neki materialni podlagi ali predstavljena digitalno [13].*

[2] *Za znani asimetrični algoritem RSA je javni ključ par števil (n,e), zasebni ključ petorček (n, p, q, e, d), kjer sta p in q naključno izbrani tuji praštevili, $n = p*q$, e tak, da velja $gcd(e,(p-1)*(q-1))=1$ in $d = e^{-1} \bmod (p-1)*(q-1)$.*

[3] *V tuji literaturi se uporablja izraz "computationally infeasible", kar pomeni, da je neko nalogo nemogoče opraviti v nekem realnem, smiselnem času, v katerem bi bil rezultat opravljene naloge še uporaben [11].*

Oseba, ki podpis preverja, dešifrira digitalni podpis s podpisnikovim javnim ključem in pridobi povzetek. Hkrati iz prejetega dokumenta z enako zgostitveno funkcijo, kot je bila uporabljena pri podpisovanju, izračuna povzetek prejetega dokumenta. Če se povzetka ujemata, je podpis overjen. Težava nastane, ko mora prejemnik sporočila ugotoviti, ali za preverjanje uporabljeni javni ključ res pripada podpisniku. Rešitev je v digitalnem potrdilu, ki vsebuje javni ključ, njegovo verodostojnost pa potrdi zaupanja vredna tretja oseba (angl. trusted third party – TTP). Digitalno potrdilo je skupek podatkov, ki najpogosteje vključuje osebne ali identifikacijske podatke lastnika, javni ključ, rok veljavnosti in dodatne tehnične podatke in ga je digitalno podpisal t. i. overitelj digitalnih potrdil (angl. certification authority – CA). Prav tako vključuje identifikacijske podatke overitelja. Digitalno potrdilo je identifikacijski dokument digitalnega sveta, tako kot je npr. osebna izkaznica identifikacijski dokument analognega sveta. Če oseba, ki preverja veljavnost digitalnega podpisa, zaupa overitelju digitalni potrdil, zaupa torej podatkom v digitalnem potrdilu in tako zaupa verodostojnosti javnega ključa, ki ga uporablja za preverjanje digitalnega podpisa. Da bi uporabnik lahko zaupal overitelju, mora zaupati njegovemu digitalnemu potrdilu. Overitelji se lahko povezujejo v različne hierarhične ali drugačne strukture, kjer je najpogosteje eden med njimi korenski overitelj, torej najvišja instanca, potrebna absolutnega zaupanja. Če je overitelj del hierarhije, je njegovo digitalno potrdilo podpisano od overitelja z višje ravni hierarhije, ki mu mora uporabnik ravno tako zaupati. Ker uporabnik ne more preveriti verodostojnosti digitalnega potrdila korenskega overitelja, saj je sam sebi podpisan, mora korenski overitelj objaviti svoje digitalno potrdilo, torej svoj javni ključ na zaupanja vreden način, npr. v znanem časopisu, v splošno razširjenih programih, kot so spletni brskalniki, ali programih za elektronsko pošto svetovno znanih proizvajalcev.

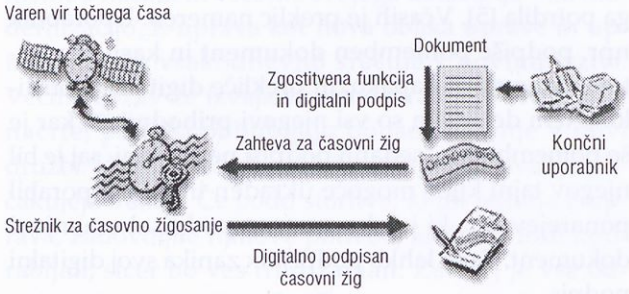
Vsak uporabnik, ki želi uporabljati digitalne podpise, mora torej dobiti digitalno potrdilo od overitelja. Overitelji so državne ali mednarodne javne ali zasebne organizacije. Ob izdaji digitalnega potrdila digitalno podpišejo podatke o lastniku in njegov javni ključ in s tem jamčijo za verodostojnost teh podatkov.

Vsako digitalno potrdilo ima časovno omejitev, t. i. rok veljavnosti (tudi korensko digitalno potrdilo korenskega overitelja). Ko rok veljavnosti poteče, digitalni podpis, izdelan in overjen z javnim ključem iz pretečenega digitalnega potrdila, ni več veljaven. To je med drugim varnostni ukrep zaradi novih tehnologij in vedno hitrejših računalnikov, ki se bodo pojavljali v prihodnosti. Če bi bilo digitalno potrdilo trajno, bi bilo namreč mogoče čez nekaj desetletij z osebnim računalnikom tistega časa v kratkem času s poizkušanjem ugotoviti ključ in ponarejati podpise. Zato vsi digitalni podpisi, izdelani po preteku digitalnega potrdila, niso več veljavni. Še več, vsi obstoječi digitalni podpisi postanejo neveljavni. To velja tako za uporabniška digitalna potrdila, kot tudi za digitalna potrdila overiteljev. Ker so digitalna potrdila lahko tudi preklicana, npr. zaradi ogrožene varnosti ali kraje tajnega ključa, velja enako tudi ob preklicu digitalnega potrdila [5]. Včasih je preklic nameren. Uporabnik npr. podpiše pomemben dokument in kasneje ugotovi, da je storil napako, in prekliče digitalno potrdilo. S tem dejanjem so vsi njegovi prihodnji in, kar je še pomembnejše, sedanji podpisi neveljavni, saj je bil njegov tajni ključ mogoče ukraden in ga je uporabil ponarejevalec, ki je zlonamerno podpisal omenjeni dokument. Tako lahko podpisnik zanika svoj digitalni podpis.

Časovno žigosanje

Kot lahko vidimo iz zgornjega besedila, je časovna komponenta pomemben dejavnik v primeru digitalnega podpisovanja. Poleg tega lahko iz izkušenj pri uporabi papirnih dokumentov ugotovimo, da ima skoraj vsak uradni dokument časovni zaznamek (datum), ki pove, kdaj je dokument nastal ali kdaj je bil podpisan. Enake potrebe se pojavljajo v primerih elektronskih dokumentov. Včasih lahko zaupamo datumu v dokumentu, ker tako trdi zaupanja vredna oseba, vendar v določenih primerih to ni dovolj. Treba je zagotoviti varen in zanesljiv zapis časa, ki je pripet na podatke ali kako drugače povezan s podatki in določa, da so podatki v takšni obliki obstajali v tistem trenutku ali prej. To dosežemo s časovnim žigom. Časovni žig je dodatek k dokumentu, zapisanem v elektronski obliki, ki določi čas obstoja, medtem ko digitalni podpis določi avtorja in vsebino. Je digitalno podpisan par podatkov – čas in povzetek dokumenta (ali digitalni podpis dokumenta) s strani overitelja časovnih žigov. Za časovno žigosanje obstaja več metod, ki omogočajo določiti, da je dokument obstajal v določeni obliki v določenem času (ne pa, kdaj je nastal). Včasih časovni žig omogoča le določitev časovnega zaporedja, tj. ali je dokument A obstajal pred dokumentom B ali

obratno. Seveda je nadvse praktično, če je zapis časa čim bliže uradno veljavnemu času, torej tistemu, ki ga uporabniki uporabljajo v vsakdanjem življenju [1]. Obstajati mora zaupanja vreden časovni vir, ki mu uporabniki zaupajo, in zaupanja vredna organizacija, ki bo ponujala tako storitev. V praksi po navadi deluje zaupanja vredna tretja oseba, imenovana overitelj časovnih žigov (angl. time stamping authority – TSA). Ponuja storitev časovnega žigosanja (angl. time stamping service – TSS). Časovni žig je torej elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času [10]. Potek žigosanja je prikazan na sliki 1.



Slika 1: **Potek časovnega žigosanja [2]**

Uporabnik napiše dokument, ga digitalno podpiše in pošlje zahtevo overitelju časovnih žigov. Ta pridobi točen čas od zaupanja vrednega vira točnega časa,[4] ga doda prispeli zahtevi in vse skupaj digitalno podpiše s svojim tajnim ključem, izdelani časovni žig pa nato vrne uporabniku. Ker overitelj časovnih žigov prejme le povzetek uporabnikovega dokumenta, je s tem zagotovljena njegova tajnost. Ker je pri postopku uporabljena tehnologija digitalnega podpisovanja, sta pri tem zagotovljena celovitost in overjanje. Uporabnik lahko preveri pravilnost časovnega žiga takoj po prejetju in s tem prepreči spregled napak pri prenosu podatkov. Zapisani čas lahko preveri in se prepriča, ali je le-ta res pravi. Preveri lahko v časovnem žigu vključeni povzetek ter tako ugotovi, da je bil časovno žigosan povzetek njegovega dokumenta.

Uporaba časovnih žigov zagotavlja overjanje digitalnih podpisov tudi za nazaj. Kot je bilo omenjeno, bi bili brez časovnega žigosanja vsi digitalni podpisi neveljavni v trenutku, ko poteče veljavnost pripadajočega digitalnega potrdila ali pa je bilo le-to preklicano. Če pa je dokument časovno žigosan, lahko oseba, ki preverja veljavnost digitalnega podpisa, preveri, ali je bil dokument podpisan pred potekom veljavnosti digitalnega potrdila, torej ko je bilo potrdilo še veljavno, ali ne.

S časovnim žigosanjem zato lahko zagotovimo nezanikanje. Čeprav se to pripisuje že uporabi digitalnih podpisov, je to napačna trditev. Le z uporabo časovnega žigosanja uporabnik namreč ne more s preklicem digitalnega potrdila zanikati digitalnega podpisa določenega dokumenta, ker s časovnim žigom lahko dokažemo, da je bilo digitalno potrdilo v času podpisovanja, torej pred preklicem ali pretekom veljavnosti digitalnega potrdila, še veljavno.

Novi znanstveni dosežki bodo v prihodnosti omogočili, da bodo že osebni računalniki hitro določili ali izračunali tajni ključ. Zatorej bi moral podpisnik podpisovati že podpisane elektronske dokumente z vedno boljšimi in varnejšimi algoritmi. Toda podpisniki pogosto sami ne arhivirajo dokumentov, ki vsebujejo podpise. Razen tega bi morali uporabniki ponovno podpisovati vse že podpisane dokumente vsakič, ko bi pretekla veljavnost njihovemu digitalnemu potrdilu in bi si pridobili novo. Z uporabo časovnega žigosanja lahko arhivarji podaljšujejo veljavnost časovno žigosanega digitalno podpisanega dokumenta s ponovnim časovnim žigosanjem obstoječih časovnih žigov[5] ob uporabi novejše in varnejše tehnologije in tako ohranijo verodostojnost originalnega digitalnega podpisa in originalnega časovnega žiga.

Overitelj časovnih žigov

Edina težava, ki ostane, je zaupanje v overitelja časovnih žigov. Rešitev je povezovalna shema časovnih žigov. Obstaja veliko različnih shem ([4], [6]), ki vse omogočajo določevanje časovnega vrstnega reda časovnih žigov in zagotavljajo, da je overitelj časovnih žigov odgovoren za svoja dejanja ali da so le-ta (pravilna ali nepravilna) dokazljiva. Povezovalne sheme temeljijo na dejstvu, da je nemogoče napovedati prihodnje zaporedje zahtev za časovne žige in povzetke,

[4] *Overitelj časovnih žigov ima lahko svoj vir točnega časa, npr. atomsko uro, ali pa uporablja več točnih virov različnih institucij po svetu, ki tak vir zagotavljajo.*

[5] *Nikoli ponovno ne žigosamo dokumenta, saj bi mu s tem dodali nov časovni žig z novim časom. Pač pa ponovno žigosamo obstoječi časovni žig in mu s tem podaljšamo veljavnost.*

ki jih bodo le-ti vključevali. Če določen časovni žig vključuje del podatkov prejšnjega, potem obstaja dokaz, da je bil tekoči časovni žig izdelan po časovnem žigu, katerega del je vanj vključen [3]. Ker bodo podatki tekočega časovnega žiga vključeni v podatke prihodnjih časovnih žigov, je zagotovljeno, da je bil tekoči časovni žig izdelan pred časovnimi žigi, nastalimi na podlagi zahtev v prihodnosti, ki vključujejo del njegovih podatkov. Taka rešitev mora seveda omogočati preveritev časovne verige žigov. V praksi se manjša časovna veriga (najpogosteje v obliki uravnoteženega Merkelejevega drevesa) izdela v nekem časovnem intervalu, npr. v eni sekundi, in torej obsega med seboj povezane podatke vseh časovnih žigov, ki so bili izdelani v tem intervalu. Skupni povzetek vseh časovnih žigov intervala se poveže s povzetkom iz prejšnjega časovnega intervala in tako tvori novo, t. i. super verigo časovnih žigov vseh intervalov. Periodično (npr. enkrat tedensko) pa se javno objavi skupni povzetek vseh povzetkov in tako izdela splošno objavljeno in nespremenljivo obliko zapisa. Javne objave tako diseminirajo in arhivirajo skupni povzetek v različnih arhivih in knjižnicah. V primeru e-uprave je medij lahko Uradni list.

Z uporabo časovnih žigov digitalno podpisani dokumenti ne pridobijo samo časovne komponente, temveč poleg obstoječe zaupnosti, celovitosti in verodostojnosti pridobijo tudi lastnost nezanikanja in mesto v času. Z uporabo povezovalnih verig ni več potrebno slepo zaupanje v overitelja časovnih žigov. Tako uporabniki pridobijo zaupanja vreden način, ki omogoča uporabo digitalnega podpisovanja in pošiljanja elektronskih dokumentov pri različnih storitvah, ki jih ponujata tako zasebni sektor kot javna uprava.

Tehnični vidiki časovnega žigosanja v upravi

Za uvajanje storitev e-uprave morajo biti izpolnjeni določeni tehnični pogoji. Najprej potrebujemo pravne podlage na področju uporabe novih tehnologij. Brez teh e-uprava ne funkcionira. Mnogo držav je že sprejelo zakone o elektronskem poslovanju ali podpisu. Ti pravni akti so se pogosto osredotočili na dve osnovni načeli, ki sta definirani tudi v direktivi Evropske unije [7], ki so jo sprejele države članice in nekatere države kandidatke. Prvo načelo določa, da elektronski podpis, ki temelji na kvalificiranem digitalnem potrdilu[6] in je izdelan z varno napravo za podpisovanje, zadošča pravnim zahtevam podpisa v odnosu do dokumentov v elektronski obliki, kot so določene za lastnoročni podpis v odnosu do papirnih dokumentov. Drugo načelo določa, da kadarkoli katerikoli drugi pravni akt omenja papirno obliko dokumenta, imamo elektronsko obliko za enakovredno in pravno veljavno, če je dostopna in uporabna za določeno časovno obdobje.

Poleg teh pa pravni akti o elektronskih in digitalnih podpisih v različnih državah vključujejo še člene o časovnem žigosanju in časovnih žigih. Večina ponudi le opise osnovnih definicij in ne posega v potrebne dodatne razlage, kot npr. avstrijski zvezni zakon o elektronskem podpisu [8] ali slovenski zakon o elektronskem poslovanju in elektronskem podpisu [10]. Drugi, kot na primer estonski zakon o digitalnem podpisu [9], natančno in jasno določajo storitev časovnega žigosanja ter overitelja časovnih žigov. Ker časovno žigosanje danes še ni spoznano kot nujni del infrastrukture javnih ključev, je pomanjkljiva pravna podlaga naloga, ki jo je treba rešiti v bližnji prihodnosti. Glede na pomanjkljivosti digitalnega podpisovanja, tj. da postanejo vsi digitalni podpisi ob preklicu ali preteku veljavnosti digitalnega potrdila neveljavni, pa različni pravni akti ponujajo različne rešitve. Slovenski zakon zahteva od podpisnika, da ponovno podpiše vse dokumente, ki jih je podpisal in se navezujejo na določeno digitalno potrdilo, ki je prenehalo veljati. Tak način reševanja je v praksi težko izvedljiv. Druga možnost, ki jo omenjajo pravni akti nekaterih držav, pa je dodajanje (overjanje) podpisov elektronskih notarjev ali pa overiteljev časovnih žigov.

Tehnološki vidik zahteva ustrezno infrastrukturo, ki omogoča izvajanje aktivnosti. Postavitev informacijske infrastrukture je zahtevna naloga in eno od temeljnih opravil, ker upošteva vse storitve, ki na njej temeljijo, torej celotno e-poslovanje. V okviru varnostnih storitev je treba poskrbeti za ustrezne postopke, ki se nanašajo tako na ponudnika kot na odjemalca. Na strani ponudnikov je treba zagotoviti zadostno število varnih spletnih strežnikov, požarnih zidov, intranetne povezave in podatkovne baze. Na strani odjemalcev pa zadostno

[6] *Izraz je uporabljen v direktivi in slovenskem zakonu o elektronskem poslovanju in elektronskem podpisu. Takšno potrdilo ima enake značilnosti kot običajno potrdilo, le da zakon zanj podrobneje predpisuje vsebino ter način izdaje, uporabe in preklica [10].*

število ponudnikov dostopa do interneta, javne dostopne točke in cenene povezave. Vse mora potekati po varnih poteh z varnimi protokoli.

Za uporabo digitalnega podpisovanja in časovnega žigosanja je treba postaviti infrastrukturo javnih ključev. Zagotoviti je treba obstoj enega ali več overiteljev, ki so lahko organizirani s strani uprave ali pa priznani in zaupanja vredni overitelji iz zasebnega sektorja. Uprave v različnih državah pogosto vzpostavijo svojega overitelja in omogočijo obstoječim in novim overiteljem zasebnega sektorja pridobitev akreditacije za izdajanje digitalnih potrdil, ki se uporabljajo pri elektronskem poslovanju z upravo. Za potrebe časovnega žigosanja pa je treba uvesti tudi overitelja časovnih žigov. Najlažji način je, da dodelimo overitelju digitalnih potrdil še možnost overjanja časovnih žigov. Določiti in vzpostaviti je treba vir točnega časa, ga povezati z overiteljevim informacijskim sistemom za izdelavo časovnih žigov in omogočiti uporabnikom časovno žigosanje njihovih dokumentov. Ker sta v takem primeru overitelj digitalnih potrdil in overitelj časovnih žigov isti organ, je treba zaupati le enemu korenskemu potrdilu, ki podpira celotno infrastrukturo. Šele po uspešno vzpostavljeni infrastrukturi lahko uprava začne ponujati varne in zaupanja vredne storitve.

Znanje je pomemben dejavnik pri ponujanju varnih e-storitev. Zato je treba prihodnje uporabnike izobraževati za uporabo informacijske tehnologije, in jim hkrati obrazložiti varnostne postopke ter tako pridobiti njihovo zaupanje v ponujene storitve. Nihče ne bo uporabljal plinskega štedilnika, če se boji plina; nihče ne bo digitalno podpisoval dokumentov, če bi ga bilo strah, da bodo lahko poneverjeni.

Primer Slovenije

Slovenija je tranzicijska država, ki poizkuša kar se da hitro doseči nivo informacijsko razvitih zahodnih držav. Hkrati se pridružuje Evropski uniji in prilagaja njenemu pravnemu redu. Slovenska vlada se trudi izpeljati spremembe učinkovito in brez večjih napak. E-uprava kot politični, ekonomski in socialni cilj je na seznamu desetih najpomembnejših nalog. Ker je bila e-uprava ena od velikih obljub zadnjih volitev, pričakujejo volivci od vlade rezultate. Slovenija je bila povabljena tudi v NATO in to je še eden od pomembnih premikov v slovenski družbi. Vse to postavlja slovensko upravo v težaven položaj.

Slovenska pravna podlaga za varno poslovanje e-uprave je bila določena leta 2000, ko je bil v skladu z direktivo Evropske unije sprejet zakon o elektronskem poslovanju in elektronskem podpisu [10]. Zakon je upošteval osnovni načeli enakosti elektronske in papirne oblike ter elektronskega in lastnoročnega podpisa, podani v direktivi EU. Tudi nekateri drugi pravni akti so morali biti spremenjeni, da niso bili v protislovju z omenjenim zakonom, da niso ovirali razvoja e-uprave in da so usklajeni s strategijo e-poslovanja uprave do leta 2004. Na določenih pravnih področjih zadeve še niso urejene.

Slovenski zakon določa časovni žig kot elektronsko podpisano potrdilo overitelja časovnih žigov, ki jamči za povezavo med dokumentom, na katerega se nanaša, in časom, vpisanim v njem. Prav tako 25. člen govori, da se za časovni žig in storitve, povezane z njim, smiselno uporabljajo določbe, ki urejajo potrdilo in kvalificirano potrdilo, vendar podrobneje ne omenja storitve časovnega žigosanja in overitelja časovnih žigov. Za resno delovanje storitve časovnega žigosanja sta omenjeni zakon in pripadajoča uredba [14] premalo.

Po sprejetju zakona [10] je bila vzpostavljena tudi infrastruktura javnih ključev. Dva korenska overitelja sta bila vzpostavljena na Centru vlade za informatiko. Prvi, SIGOV-CA, izdaja digitalna potrdila za zaposlene v javni upravi in drugi, SIGEN-CA, za uporabnike, tj. državljane in zasebni sektor. Zaposleni v javni upravi so ponekod pridobili tudi naprave za uporabo pametnih kartic, medtem ko morajo uporabniki to težavo reševati sami.

Trenutno v Sloveniji še nimamo overitelja časovnih žigov za področje e-storitev uprave. Na Centru vlade za informatiko imajo vir točnega časa in uporabljajo rešitve podjetja Entrust, ki je eden vodilnih proizvajalcev na svetu. Njegove rešitve vključujejo tudi možnost vzpostavitve overitelja časovnih žigov, kar je ena od možnih rešitev za slovensko e-upravo. Po zadnjih podatkih naj bi bila ta rešitev tudi izpeljana in v določeni meri funkcionalna še letos.

Spletni portal e-uprava je postavljen in že nekaj časa ponuja prve storitve e-uprave ob uporabi digitalnih potrdil omenjenih overiteljev. Nekatere od teh storitev so na voljo brezplačno, čeprav mora zanje državljan, če jih opravi po normalni (neelektronski) poti, plačati takso. Storitev omogoča uporabnikom pridobitev izpiskov iz matičnih knjig in vpogled v

centralni register prebivalstva ob uporabi digitalnega potrdila, ki omogoča overjanje in identifikacijo uporabnika. Zaposleni, ki delajo v organih uprave in predstavljajo ponudnika storitev, uporabljajo digitalna potrdila za dostop do podatkovnih baz, ki vsebujejo vloge uporabnikov po izpiskih in te vloge rešujejo. Rezultat teh postopkov je izpis na papirju, ki ga naročnik prejme po pošti. Slaba stran tega je, da je bila ta storitev vpeljana zaradi političnih predvolilnih obljub. Od takrat se je v okviru ponujenih storitev zgodilo zelo malo. Še slabše: izpiski, pridobljeni po elektronski poti in dostavijo v papirni obliki, se ponovno uporabljajo kot priloge papirnim vlogam za postopke v javni upravi.

Trenutno za končnega uporabnika še ne obstaja storitev, ki bi uporabljala digitalne podpise ali časovne žige. Podobna situacija obstaja v mnogih drugih državah, kjer digitalna potrdila uporabljajo za overjanje in identifikacijo, medtem ko je storitev, ki uporabljajo digitalni podpis ali časovni žig, malo ali pa jih sploh ni. Vendar kaže, da bo že dolgo pričakovana e-dohodnina prvi korak v tej smeri in bo na voljo že v prihodnjem letu.

Smo pripravljeni?

Nedavno so predstavniki skupine GartnerGroup na svoji spletni strani objavili, da mnogi projekti uvajanja e-storitev v upravi ne pomagajo niti državljanom niti upravi sami. Ne samo, da politične obljube o manjših stroških z manj zaposlenimi v sodobnih upravah niso uresničljivi zaradi močnih sindikatov in strahu pred povečano nezaposlenostjo v državi, temveč tudi hitro uvajanje slabih e-storitev doseže slab učinek pri uporabnikih. Vse prepogosto so take e-storitve kompleksne in jim uporabniki ne zaupajo.

Več kot 6000 izdanih digitalnih potrdil za državljane slovenskega overitelja na Centru vlade za informatiko obljublja uporabo e-storitev, vendar bodo brez časovnega žigosanja državljani ta digitalna potrdila lahko uporabljali le za identifikacijo. Ko bo treba podpisovati vloge, priloge, elektronska sporočila, pa bo treba zagotoviti časovno žigosanje, ki bo poleg zagotavljanja nezanikanja omogočalo tudi varno in dolgoročno zagotavljanje verodostojnosti podpisov in podpisane vsebine. Le tako bo e-uprava uspela pridobiti zaupanje uporabnikov in vpeljati sodobne e-storitve kot mnoge razvite države v svetu.

Literatura

1. Admas, C., Lloyd, S.: Understanding Public-Key Infrastructure. Macmillan Technical Publishing, Indiana ZDA (1999).
2. Entrust: Entrust/Timestamp, URL="http://www.entrust.com/ entrust/timestamp/ index.htm" (2001).
3. Bayer, D., Haber, S., Stornetta, W. S.: Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences II: Methods in Communication, Security, and Computer Science. Springer-Verlag, Berlin, Heidelberg, New York (1993) 329–334.
4. Buldas, A., Laud, P., Lipmaa, H., Villemson, J.: Time stamping with binary linking schemes. Advances in Cryptology – CRYPTO'98, LNCS 1462. Springer-Velrag, Berlin Heidelberg New York (1998) 486-501.
5. Maniatis, P., Baker, M.: Enabling the archival storage of signed documents, Computer Science Department, Stanford University, 24th July 2001.
6. Benaloh, J., de Mare, M.: Efficient Broadcast time-stamping. Technical report 1, Clarkson University Department of Mathematics and Computer Science (1991).
7. European Community: A European Initiative on Electronic Commerce. COM(97) 157 (1997).
8. Austrian Federal Electronic Signature Law (Signature Law - SigG) (2000).
9. Tõlge inglise keeled: Eesti Õigustõlke Keskus, Estionian Digital Signatures Act, (RT I 2000, 26, 150), Estonian Legal Translation Centre (2000). URL="http://www.riik.ee/riso/digiallkiri/digsignact.rtf".
10. Zakon o elektronskem poslovanju in elektronskem podpisu. Uradni list Republike Slovenije, 57/2000 (2000).
11. American Bar Association: Digital Signature Guidelines (1997).
12. Lenk, K., Traunmüller, R., Electronic Government: Where Are We Heading? Lecture Notes in Computer Science, Springer-Verlag Heidelberg. Volume 2456/2002, Electronic Government: First International Conference, EGOV 2002, Aix-en-Provence, France, September 2–5, 2002. Proceedings.
13. Gladney, H.M., Digital documents Quarterly, Glossary and acronyms, URL="http://home.pacbell.net/hgladney/ ddqgloss.htm" (2003).
14. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. Ur. list RS, št.77/2000, 2/2001.

Mag. Mitja Dečman je leta 2001 končal magistrski študij na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zaposlen je kot asistent na Fakulteti za upravo v Ljubljani, kjer se poleg pedagoškega dela na področju informatike v upravi ukvarja še z raziskavami s področja varnosti informacijskih sistemov, infrastrukture javnih ključev in elektronskih storitev v javni upravi.

Dr. Marjan Krisper je predstojnik katedre za informatiko na Fakulteti za računalništvo in informatiko in od ustanovitve leta 1992 predstojnik Laboratorija za informatiko. Je član več znanstvenih in strokovnih združenj, med drugim ustanovitveni član AIS (Association for Information Systems) – svetovne zveze univerzitetnih učiteljev informacijskih sistemov, Slovenskega društva INFORMATIKA, Društva za umetno inteligenco in INFOS-a. Je avtor številnih raziskav, elaboratov, ekspertiz, znanstvenih in strokovnih sestavkov. Vodi številne projekte razvoja informacijskih sistemov in izvajanja metodologij razvoja v največjih sistemih v gospodarstvu, državni upravi in javnem sektorju.

Vzorci in prakse: kako izboljšati varnost .NET aplikacij

Leon Grabenšek, Microsoft
leong@microsoft.com

Povzetek

Vzorci in prakse je naziv za skupek referenčnih arhitektur, gradnikov, praks in vzorcev visoko kvalitetne programske kode in najboljših praks, ki jih je zbral Microsoft in so plod sodelovanja notranjih in zunanjih, neodvisnih sodelavcev. Vzorci in prakse so izvrstno orodje za upravljanje varnostnega tveganja rešitev v ASP.NET. Vložek za uporabo je predvsem v izobraževanju, pridobljene dobrine pa v boljšem obvaldovanju tveganja, krajšem času izvedbe projektov, večji kvaliteti in ponovljivosti projektov.

Abstract

Patterns and Practices: How to improve security risk of .NET applications

Patterns and practices is a common name for a cluster of reference architecture, building elements, practices and patterns of high quality programme code as well as the best practices which were collected by the Microsoft and which represent the result of cooperative work of inner and outer independent professionals. Patterns and practice are an outstanding tool for managing security risks solutions in ASP.NET. Training is the most important investment regarding the usage, but the benefits you gain are shorter implementation time, better quality and feasability to multiply a project.

Namen in uporaba vzorcev in praks

Vzorci in prakse je naziv za skupek referenčnih arhitektur, gradnikov, praks in vzorcev visoko kvalitetne programske kode in najboljših praks, ki jih je zbral Microsoft in so plod sodelovanja notranjih in zunanjih, neodvisnih sodelavcev. Objavljeni so na Microsoftovih spletnih straneh in so brezplačno dostopni vsakomur.

Vzorci in prakse so se začeli zbirati, ko so izkušeni programerji pri delu na več projektih opazili, da se zasnove določenih rešitev ponavljajo. Nato so začeli te zasnove opisovati kot pripomoček in priročnik. Vsak vzorec in praksa je plod dela več avtorjev in programerske skupnosti; tako se je izboljšala kvaliteta, uporabnost in neodvisnost vzorcev in praks.

Vzorci in prakse obsegajo zelo širok spekter področij. Metodologija se dotika vseh faz procesnega modela po Microsoft Solutions Framework (MSF) in delno Microsoft Operations Framework(MOF). To pomeni, da je pokrit celoten razvoj in vzdrževanje .NET aplikacij.

Prednosti uporabe vzorcev in praks za podjetja

Podjetja imajo od vzorcev in praks koristi, ki se hitro lahko izrazijo v številkah in datumih uspešnih projektov.

Obvladovanje tveganja

Z uporabo vzorcev in praks se zmanjšujejo neznanke in s tem podjetja laže obvladujejo tveganja projektov.

Čas izvedbe

Čas, potreben za izvedbo projektov, je krajši, saj projekti gradijo na že ustvarjenem znanju.

Kvaliteta in dodana vrednost

Kvaliteta je vgrajena v vzorce in prakse in jo z njihovo uporabo sprejemamo, izvajalec se lahko bolj osredotoči na poslovno stran projekta in s tem dodatno poveča njegovo kvaliteto in doda vrednost.

Ponovljivost

Vzorci in prakse temeljijo na rešitvah v realnem svetu. Napisani so tako, da so uporabni za kogarkoli z podobno poslovno zahtevo. Odstranjene so posebnosti posameznih strank. Tako se poveča ponovljivost in uporabnost. Vložek v izobraževanje bo obrodil sad pri izvedbi naslednjih projektov, ker bo znanje o zasnovah in know-how že pridobljeno.

Pregled vzorcev in praks, s katerimi povečamo varnost .NET aplikacij

Vzorci in prakse so zbrani po vsebinskih sklopih; eden od njih je tudi varnost .NET aplikacij.

Tako faze procesnega modela MSF, ki se nanaša na razvojne projekte, kot MOF, ki se nanaša na vzdrževanje in upravljanje sistemov. V tem prispevku jih bomo razdelili na razvojne in vzdrževalne sklope.

Razvoj

V nadaljevanju si bomo ogledali, katere vsebine pokrivajo vzorci in prakse v okviru razvoja .NET aplikacij.

Building Secure ASP.NET Applications

Opisan je varnostni model aplikacij ASP.NET. Poglobljeno je opisano različno overjanje prijave in določanje pooblastil.

Poleg različnih konceptov je knjiga polna konkretnih in uporabnih receptov, ki zelo natančno opisujejo, kako se kaj naredi (klikni na ..., odpri ..., dodaj kodo ...).

Vsebovano je pregledno kazalo receptov, kako se izdela posamezna funkcionalnost, npr. kako poklicati spletno storitev z uporabo SSL. Vsebovani so tudi vzorčni primeri programske kode.

Knjiga se ukvarja še z varno komunikacijo in varnostjo v intranetu, ekstranetu, internetu, varnostjo v ASP.NET, Enterprise Services, spletnih storitvah, rešitvah .NET Remoting ter varnostjo dostopa do podatkov.

Improving Web Application Security: Threats and Countermeasures

Opisuje varnostne pretnje in protiukrepe. Včasih podjetja živijo v miselnosti, da je za varnost dovolj požarni zid, vendar to žal ne drži. Za varnost aplikacij je potrebno več, kot je opisano v teh gradivih.

Leta 2002 je spletni časopis eWeek sponzoriral izziv, kjer je Microsoftova razvojna skupina zgradila ASP.NET aplikacijo na Windows 2000 in platformi .NET, treba pa je bilo vdreti v to aplikacijo. Zabeležili so 82.500 poskusov vdora v aplikacijo, nobeden pa ni bil uspešen. Med mnogimi tehnikami zaščit je opisana tudi ta aplikacija.

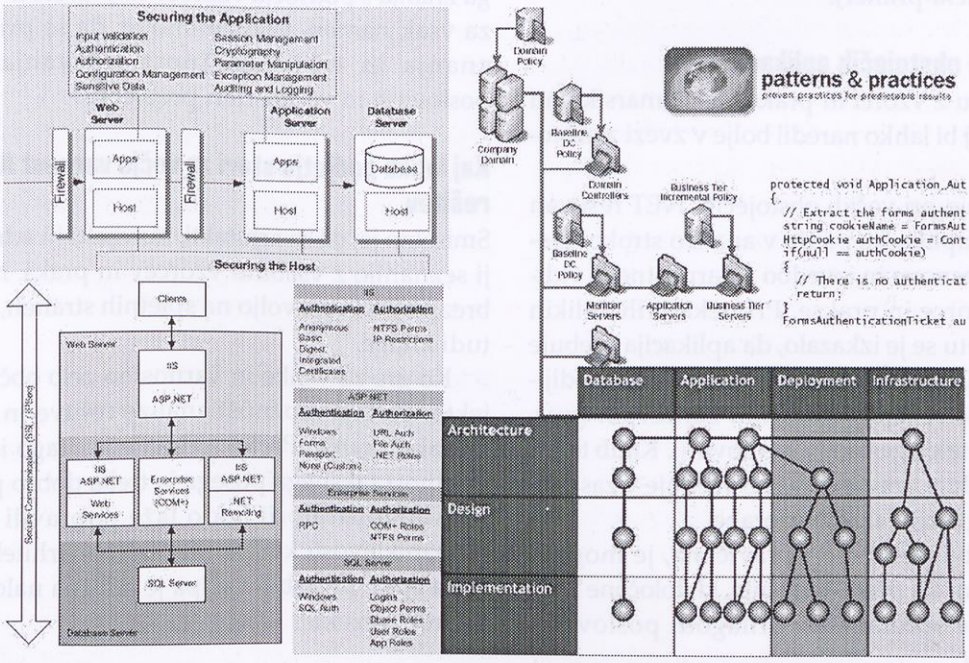
Opisani so temelji varnostne zaščite, kako se izvajajo napadi in načini določanja pretenj. Določi se arhitektura varne spletne aplikacije. Opisan je razvoj varne ASP.NET aplikacije ter zagotavljanje varnosti različnih strežnikov. Razložen je način, kako preveriti varnost v programski kodi in sami postavitvi.

Designing Application-Managed Authorization

Opisani so osnovni koncepti dodeljevanja pooblastil. Kje in kdaj izvesti dodeljevanje pooblastil v nivoju uporabniškega vmesnika, poslovnem in podatkovnem nivoju ter različni načini izvedbe z .NET varnostnimi vlogami. Priročnik v prilogi vsebuje primere izvedbe.

Authentication in ASP.NET: .NET Security Guidance

Spletna stran se ukvarja z različnimi načini in scenariji overjanja prijave v ASP:NET aplikaciji. Za vsak način je opisano, kdaj je primeren in kdaj ne.



Slika 1: **Vzorci in prakse povečujejo varnost**

Vzdrževanje

Tudi administratorji sistemov lahko pridobijo iz vzorcev in praks. V nadaljevanju je na kratko povzeta vsebina iz priročnikov o vzdrževanju.

Deploying .NET Framework-based Applications

Opisuje različne tipe .NET aplikacij in strukturo ter možnosti namestitev. Ob tem se dotika tudi varnostnih tematik pri pripravi okolja aplikacije, namestitvi in vzdrževanju.

Operating .NET-based Applications

Priročnik je razdeljen na tri glavne vsebine, in sicer s področja nadzora, varnosti ter načrtovanja zmogljivosti. Za lažjo predstavo so primeri v dokumentu narejeni na osnovi vzorčne aplikacije.

Poglavje o varnosti obsega:

- splošna varnostna priporočila (npr. redno nameščanje popravkov),
- upravljanje varnosti s pravilniki skupin v Windows 2000,
- zaščito strežnikov glede na vlogo v aktivnem imeniku (npr. krmilnik domen),
- zaščito strežnikov, na katerih tečejo .NET aplikacije,
- komunikacijo med .NET aplikacijami na dislociranih strežnikih in odjemalcih (npr. SSL),
- priredbo varnostnega okolja določeni .NET aplikaciji (praktični primer).

Prefaktoriranje obstoječih aplikacij

Ob spoznavanju z vzorci in praksami se marsikomu porodi ideja, kaj bi lahko naredil bolje v zvezi z obstoječo aplikacijo.

Podjetja imajo pri večjih obstoječih .NET rešitvah možnost, da se aplikacija preda v analizo strokovnjaku, ki preveri zasnovo in izvedbo z varnostnega vidika glede na vzorce in prakse. Pri nekaterih velikih strankah po svetu se je izkazalo, da aplikacija vsebuje rešitve, ki z vidika varnosti (ali velikostne prilagodljivosti itd.) ne ustrezajo poslovnim zahtevam (npr. nešifriran piškotek z geslom v e-trgovini). Kljub temu da aplikacija deluje pravilno, lahko vsebuje v zasnovi luknje, ki omogočajo različne zlorabe.

Če je naložba poslovno upravičena, je mogoče pristopiti k postopku prefaktoriranja, ki določene koncepte aplikacije spremeni in prilagodi poslovnim zahtevam. Scenarij uporabe aplikacije ostane enak.

Tu lahko pomaga metoda ekstremnega programiranja z vnaprejšnjim testiranjem, po kateri se vnaprej napišejo testi aplikacije, ki se s posebnim programom sprožijo po vsaki spremembi v programski kodi. Programer, ki prefaktorira aplikacijo, sproti izve, ali so njegove spremembe programske kode vplivale na pravilnost delovanja. Skrajša se čas stabilizacije aplikacije in poveča njena kvaliteta. Slabost tega pristopa je, da je že pred začetkom prefaktoriranja treba napisati precej testov, hkrati pa je težko presoditi, kdaj je testov dovolj (še vedno je potreben klasičen postopek testiranja, ki pa je v tem primeru krajši, saj najde manj napak).

Problematika vzorcev in praks

Vzorci in prakse obsegajo skupek možnih rešitev. Seveda ni vsaka rešitev primerna za vsako poslovno zahtevo; nekateri vzorci so kompleksnejši in rešujejo bolj zahtevne poslovne probleme.

Zgodilo se je že, da se je arhitekt ali razvijalec uspešno naučil in uporabil določen zahtevnejši vzorec ali prakso. Ker je bilo znanje že pridobljeno, je bilo najbolj enostavno že znano rešitev uporabiti tudi v naslednjih projektih. Na ta način so bile izdelane aplikacije včasih po nepotrebnem kompleksnejše, kot je bilo definirano z vidika poslovnih zahtev.

Zato je potrebno stalno nadgrajevanje pridobljenega znanja s področja vzorcev in praks. Ni vsak vzorec za vsak namen. Pomembno je, da se pridobi širina znanja in tako zmožnost reševanja različnih poslovnih in varnostnih problemov.

Kaj lahko podjetje stori za večjo varnost ASP.NET rešitev

Smiselno je, da se arhitekti, razvijalci in administratorji seznanijo z vsebino vzorcev in praks. Materiali so brezplačni in na voljo na spletnih straneh, na voljo so tudi knjige.

Ko gre za velike in varnostno zelo občutljive projekte, obstaja možnost analize rešitve in po potrebi prefaktoriranje. Prefaktoriranje je drago in poslovno vrednost takšnega posega je treba dobro pretehtati.

Administratorji bodo laže popravili morebitne pomanjkljivosti kot pa razvijalci in arhitekti. Znanje, ki ga bodo pridobili vsi, pa je odlična naložba za prihodnje projekte.

V primeru, da je podjetje naročnik rešitve, lahko izrazi željo izvajalca po skladnosti rešitve z vzorci in praksami ali vsaj obrazložitev, kateri vzorci in prakse so uporabljeni.

Sklep

Vzorci in prakse so izvrstno orodje za upravljanje varnostnega tveganja rešitev v ASP.NET. Vložek za uporabo je predvsem v izobraževanju, pridobljene dobrine pa v boljšem obvladovanju tveganja, krajšem času izvedbe projektov, večji kvaliteti in ponovljivosti projektov.

Literatura in viri

Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/secnetlpMSDN.asp

Improving Web Application Security: Threats and Countermeasures
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp

Authentication in ASP.NET: .NET Security Guidance
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnbda/html/authaspdotnet.asp

Designing Application-Managed Authorization
http://msdn.microsoft.com/library/?url=/library/en-us/dnbda/html/damaz.asp

Deploying .NET Framework-based Applications
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnbda/html/DALGRoadmap.asp

Operating .NET-based Applications
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/net/maintain/opnetapp/default.asp

MSF
http://www.microsoft.com/msf

MOF
http://www.microsoft.com/mof

Leon Grabenšek je magistriral na Fakulteti za računalništvo in informatiko v Ljubljani. Ima devetletne izkušnje na uspešno zaključenih projektih kot vodja razvoja (MAOP, d. o. o.), razvijalec in administrator baz podatkov (Blagovna borza, d. d.) s področja razvoja in administracije aplikacij in baz podatkov na vsebinah ERP in borznih sistemov. Znanje in izkušnje deli z drugimi tudi kot predavatelj in pisec člankov. Sedaj kot svetovalec pri slovenskem Microsoftu svetuje večjim slovenskim podjetjem pri uporabi ustreznih rešitev, razvitih z Microsoftovimi tehnologijami, in predava na različnih srečanjih in konferencah.

Upravljanje IT infrastrukture – ITIL in MOF

Primož Karlin, Microsoft, d. o. o.
pkarlin@microsoft.com

Povzetek

Prispevek podaja kratek opis težav, ki jih pri upravljanju in obratovanju IT sistemov in rešitev pogosto srečujejo podjetja, ter pregled v svetu uveljavljenih pristopov za njihovo reševanje: ITIL – Information Technology Infrastructure Library ter MOF – Microsoft Operations Framework. Podrobneje je opisan MOF, njegovi moduli, proces in organizacija.

Abstract

Managing IT infrastructure – ITIL in MOF

The paper shortly discusses the problems companies are facing while managing and operating of IT infrastructure and solutions. It also gives an overview of standard solutions in this field: ITIL – »Information Technology Infrastructure Library" and MOF – »Microsoft Operations Framework". Further on the paper gives more in-depth overview of MOF modules, processes and organization.

Neverjetna rast, ki smo ji bili v preteklosti priča na področju informacijske tehnologije, je poleg očitnih prednosti odprla tudi nove probleme. V 90. letih prejšnjega stoletja je bila glavna naloga IT organizacij in oddelkov čim hitrejše uvajanje novih funkcionalnosti – stroški in učinkovitost niso bili glavno merilo uspešnosti. Cilj je bil čim hitrejša uvedba novih storitev in funkcionalnosti. Delovanje IT organizacij in oddelkov je bilo reaktivno in ne proaktivno. Časa za načrtovanje in koordinacijo je bilo (pre)malo.

V podjetjih investicije in stroški v informacijsko tehnologijo prav gotovo predstavljajo nezanemarljivo postavko. Glede na trenutni ekonomski položaj podjetij je upravljanje IT infrastrukture dobilo nov, večji pomen.

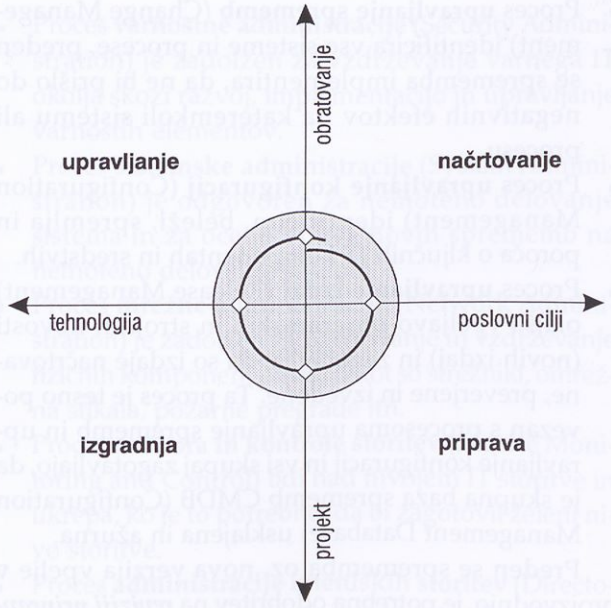
Da bi bili projekti na področju informacijske tehnologije čim uspešnejši, je Microsoft v drugi polovici 90. let prejšnjega stoletja izdal navodila kako učinkovito načrtovati, razviti, implementirati, upravljati in podpirati takšne rešitve – predvsem na Microsoftovih produktih. Navodila so dovolj splošna, da jih je mogoče uporabiti za vsako IT okolje. Organizirana so v dva komplementarna sklopa – ogrodji: ogrodje rešitve (Microsoft Solutions Framework – MSF) in ogrodje upravljanja in obratovanja (Microsoft Operations Framework – MOF). Ob uvedbi storitev, ki temeljijo na IT tehnologiji, je treba:

- razumeti potrebe in na podlagi tega ustvariti rešitev in
- upravljati dobljeno rešitev, da zagotovimo želeni nivo storitev.

Tako sta zasnovani tudi ogrodji – MSF se loteva prve, MOF pa druge. Ogrodji sta bili zasnovani tako, da bi bil čas med identifikacijo novih potreb (storitev) in trenutkom, ko so na voljo, čim krajši. Vsako ogrodje daje navodila in informacije o ljudeh, procesih in tehnologijah, ki jih potrebujemo za uspešno zagotavljanje IT storitev. Slika 1 prikazuje, kako v Microsoftu definiramo cikel vpeljave IT storitev in rešitev ter kje sta umeščeni ogrodji MSF in MOF. V obeh ogrodjih je uporabljena tudi dosledna terminologija in koncepti, kar zagotavlja manjšo porabo časa in višjo kakovost informacijskih storitev, ki jih dobimo kot rezultat. Ob uporabi MSF in MOF ogrodij postane usmeritev IT organizacij in oddelkov učinkovitost in ne hitrost – poudarek je na storitvah in ne na produktih. Paradoksalno pa je, da s takim pristopom, ko si vzamemo čas za implementacijo konsistentnosti in kolaboracije v procese, čas v resnici prihranimo in rešitve implementiramo hitreje.

Upravljanje in ogrodje MOF

Trenutno je v svetu na področju upravljanja informacijskih sistemov eden najbolj priznanih standard ITIL (Information Technology Infrastructure Library), saj ga uporabljajo in priporočajo vsa večja svetovna računalniška podjetja, kot so Microsoft, HP, IBM idr. V resnici gre za skupek dokumentov, ki povzemajo najboljše izkušnje, do katerih so prišla podjetja in organizacije pri upravljanju IT. ITIL je nastal v Angliji pod okriljem CTTA (Central Computer and Telecommunications



Slika 1: **IT cikel**

Agency) v 80. letih dvajsetega stoletja, danes pa za nadaljnji razvoj skrbi OCG (Office of Government Commerce). Prvotna usmeritev ITIL-a je bilo upravljanje informacijske infrastrukture v angleških vladnih ustanovah, danes pa se uporablja po vsem svetu kot eden od standardov v gospodarstvu in negospodarstvu. ITIL se predvsem ukvarja s »kako« in ne »s čim«. Pri Microsoftu pa smo šli korak dlje; ogrodje MOF se v celoti naslanja na ITIL, vendar daje usmeritve in navodila tudi na področju »s čim« – katera orodja in tehnologije uporabiti za zagotavljanje visokega nivoja IT storitev. MOF tako na podlagi ITIL in izkušenj Microsoftovih partnerjev, strank, interne IT organizacije in Microsoft Services organizacije zagotavlja:

- uporabo rešitev in zamisli, ki dokazano delujejo v praksi,
- znanje in informacije za uspešno upravljanje IT rešitev,
- definicijo procesov, tehnologij in ljudi, ki so za to potrebni,
- povečanje prilagodljivosti IT za boljše in hitrejše prilagajanje podjetij in ustanov na spremembe,
- integracijo z MSF ogrodjem za uspešnost celotnega cikla IT okolij in
- usmeritev na storitve in ne na strežnike in tehnologijo.

Pokažimo na primeru, ko se v podjetju uporabniki elektronske pošte pritožijo nad slabo odzivnostjo sistema. IT oddelek, ki ne uporablja MOF in je usmerjen v izdelke, bo k reševanju tega problema pristopil s testiranjem in diagnostiko vseh posameznih komponent sistema (mreža, strežniki, programska oprema itd.). Uporabnikov pa v resnici ne zanima, ali vsaka posamezna komponenta sistema deluje pravilno, zanima jih nivo in kakovost storitve – elektronske pošte. In s takšnim pogledom in načinom razmišljanja se bo ukvarjal IT oddelek, ki uporablja MOF.

Modeli MOF

MOF je zgrajen okrog treh področij – modelov:

- procesnega (Process Model),
- skupinskega (Team Model) in
- modela tveganj (Risk Model).

Na teh področjih daje MOF usmeritve o procesih, ljudeh in upravljanju s tveganji pri IT storitvah. Vsako področje je zgrajeno na izkušnjah, dokazano delujočih primerih in tehnologijah, ki so nam lahko v pomoč pri implementaciji. Z vsakim posameznim področjem in njihovo kombinacijo pa dosežemo večjo razpoložljivost, zanesljivost IT sistemov, dobimo pa tudi navodila za vzdrževanje in upravljanje.

Procesni model

Procesni model predstavlja funkcionalni del procesov, ki jih izvajamo pri vzdrževanju in upravljanju IT storitev. Temelji na štirih principih:

- **Strukturirana arhitektura**. Strukturiranje vseh aktivnosti znotraj obratovanja in upravljanja IT sistema.
- **Hiter življenjski cikel, iterativne izboljšave**. Tempo, s katerim se IT sistemi spreminjajo, se povečuje in je rezultat hitrega tehnološkega razvoja in potrebe poslovnih okolij po inovativnosti in konkurenčnosti. MOF za reševanje tega problema predstavlja koncept iterativnega življenjskega cikla, ki zagotavlja hitro vpeljavo sprememb in izboljšav ter stalno spremljanje in izboljševanje IT storitev.
- **Pregledi in revizije**. Procesni model vsebuje preglede v ključnih točkah življenjskega cikla, v katerih ocenimo rezultate in učinkovitost. Te revizije dajejo možnost, da so vodstvene strukture v podjetjih vpletene v procese, ko je to najbolj potrebno.
- **Upravljanje s tveganji**. Obratovanje IT sistemov postaja vse pomembnejše in bolj zapleteno in napake in izpadi so vse bolj vidni in boleči tako za kupce in stranke kot tudi za notranje uporabnike. Pomen upravljanj s tveganji je zato ključen.

MOF procesni model opisuje življenjski cikel, ki ga lahko uporabimo za poljubne storitve. Prav tako ga lahko uporabimo za različne velikosti rešitev – od najmanjših do največjih. Slika 2 prikazuje življenjski cikel, kvadrante in preglede – revizije, omenjene v prejšnjem odstavku.

Poglejmo, kako so povezani kvadranti MOF procesnega modela v spiralni življenjski cikel. Še prej pa moramo razložiti, kaj so gradniki, ki jih uporabljamo v kvadrantih. V vsakem kvadrantu nastopajo procesi, ki stremijo k istemu cilju – recimo spreminjanje ali obratovanje. Procese v modelu MOF imenujemo SMF (Service Management Functions) in jih je dvajset (npr. upravljanje sprememb, upravljanje zmožnosti itd.).

Vzemimo, da je IT storitev trenutno v točki življenjskega cikla, kjer je že odobrena, razvita, preverjena in pripravljena za namestitev v produkcijsko okolje (v resnici bi lahko začeli na poljubni drugi točki življenjskega cikla, vendar za ta primer izberimo to).

Spreminjanje

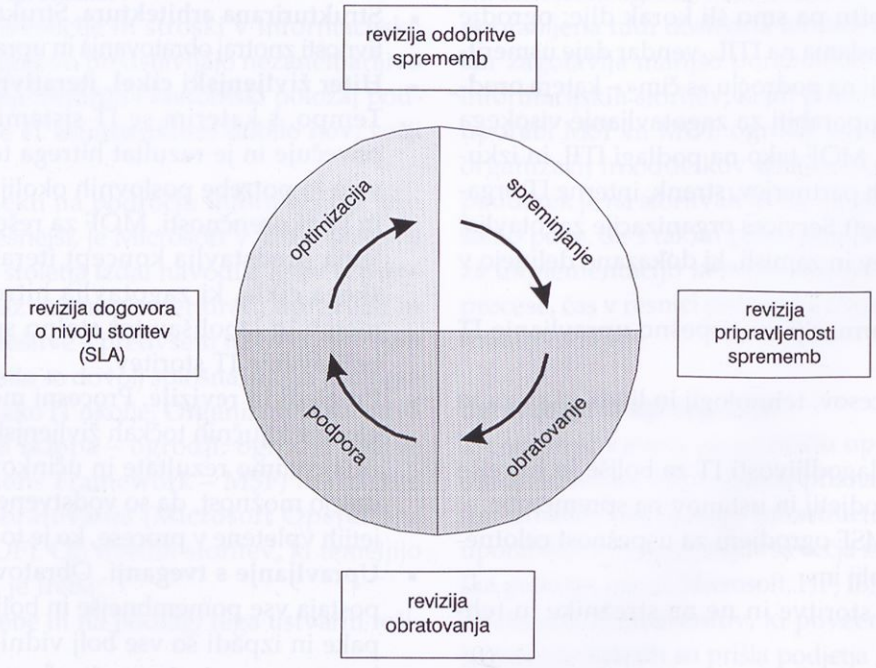
Po pregledu (reviziji) odobritve sprememb, ko so torej spremembe odobrene, in pred pričetkom razvoja in implementacije sprememb, vstopamo v kvadrant spreminjanje. Z naslednjimi procesi (SMF-ji), ki so del tega kvadranta, skrbimo za upravljanje pobude za spremembe, razvoj in namestitev le-teh:

- Proces **upravljanje sprememb** (Change Management) identificira vse sisteme in procese, preden se sprememba implementira, da ne bi prišlo do negativnih efektov na kateremkoli sistemu ali procesu.
- Proces **upravljanje konfiguracij** (Configuration Management) identificira, beleži, spremlja in poroča o ključnih IT komponentah in sredstvih.
- Proces **upravljanje izdaj** (Release Management) olajša vpeljavo programskih in strojnih novosti (novih izdaj) in zagotavlja, da so izdaje načrtovane, preverjene in izvedene. Ta proces je tesno povezan s procesoma upravljanje sprememb in upravljanje konfiguracij in vsi skupaj zagotavljajo, da je skupna baza sprememb CMDB (Configuration Management Database) usklajena in ažurna.

Preden se sprememba oz. nova verzija vpelje v proizvodnjo, je potrebna odobritev na *reviziji pripravljenosti sprememb*. Po implementaciji spremembe pa pregled oceni in ugotovi uspešnost spremembe in njeno efektivnost ter efektivnost celotnega procesa spreminjanja.

Obratovanje

Po uspešni uvedbi spremembe v proizvodnji preidemo v fazo obratovanja, v kateri naslednji procesi (SMF-ji) skrbijo za vsakodnevne aktivnosti:



Slika 2: **Procesni model MOF**

- Proces **varnostne administracije** (Security Administration) je zadolžen za vzdrževanje varnega IT okolja skozi razvoj, implementacijo in upravljanje varnostih elementov.
- Proces **sistemske administracije** (System Administration) je odgovoren za nemoteno delovanje sistema in za oceno vpliva novih sprememb na nemoteno delovanje sistema.
- Proces **mrežne administracije** (Network Administration) je zadolžen za načrtovanje in vzdrževanje fizičnih komponent omrežja kot so strežniki, omrežna stikala, požarne pregrade itn.
- Proces **nadzora in kontrole storitev** (Service Monitoring and Control) bdi nad nivojem IT storitve in ukrepa, ko je to potrebno, da bi zagotovil želeni nivo storitve.
- Proces **administracije imeniških storitev** (Directory Services Administration) je zadolžen za dnevno obratovanje, vzdrževanje in podporo imeniku podjetja.
- Proces **upravljanje hrambe podatkov** (Storage Management) skrbi za krajevno in oddaljeno hrambo podatkov predvsem z namenom možnosti obnovitve in arhiviranja ter zagotavljanja fizičnega varovanja varnostnih kopij in arhivov.
- Proces **razporejanje opravil** (Job Scheduling) skrbi za paketno obdelavo (batch processing) ob različnih časih, za maksimalno izkoriščenost sistemskih virov.
- Proces **upravljanje tiskanja in izhoda** (Print and Output Management) skrbi za stroške in vire, povezane z izhodom ter zagotavlja varnost občutljivih izhodnih podatkov.

Revizija obratovanja se naredi periodično. Ta pregled je interno usmerjen na zmožnost zaposlenih v IT za upravljanje in vzdrževanje dane IT storitve, zagotavljanje nivoja storitve in dokumentiranje izkušenj v bazo znanja.

Podpora

Težave in problemi se prav gotovo pojavijo v vsakem IT okolju. Podporna funkcija MOF modela vsebuje naslednja procesa za hitro reševanje incidentov, problemov in poizvedb uporabnikov:

- Proces **upravljanje incidentov** (Incident Management) upravlja incident v njegovem življenjskem ciklu od odkritja in dokumentiranja do preiskave, diagnoze in rešitve.
- Proces **upravljanje problemov** (Problem Management) preiskuje in rešuje izvor problemov in napak ter ostalih motenj nivoja storitev.

Revizija dogovora o nivoju storitev (SLA) se dela periodično in oceni zmožnost zaposlenih v IT oddelku za zagotavljanje zahtevanega nivoja storitev v skladu z *dogovorom o nivoju storitev (SLA pogodba)*. Po reviziji je potrebno narediti spremembe in popravke na področjih, na katerih pregled pokaže pomanjkljivosti oz. je treba določiti (na pogajanjih) spremembe SLA pogodbe. Poleg tega pa sta procesa v tem kvadrantu gonilna sila sprememb specifičnih procesov, orodij in procedur, ki jih uporabljamo pri obratovanju.

Optimizacija

Procesi v prejšnjih dveh kvadrantih skrbijo za naloge pri vsakodnevnem obratovanju. V kvadrantu optimizacije pa imajo procesi bolj proaktiven pristop in ocenjujejo trenutne performanse ter napovedujejo bodoče potrebe. Včasih procese v ostalih kvadrantih karakteriziramo kot *obratovalne*, procese v tem kvadrantu pa *taktične*. Ti procesi so:

- Proces **upravljanje nivoja storitev** (Service Level Management) zagotavlja nivo storitev skozi pogajanja, spremljanje in vzdrževanje *dogovora – pogodbe o nivoju storitev* med ponudniki in uporabniki IT storitev.
- Proces **upravljanje zmožnosti** (Capacity Management). Načrtovanje in nadzor IT storitev in infrastrukture s stališča potrebnih virov za zagotavljanje ustreznega nivoja storitev iz prejšnje alinee.
- Proces **upravljanje razpoložljivosti** (Availability Management). Opis, upravljanje, vodenje in proaktivno vzdrževanje za zagotavljanje razpoložljivosti informacij in storitev znotraj dogovorjenih stroškovnih okvirov in *dogovora – pogodbe o nivoju storitev*.
- Proces **finančno upravljanje** (Financial Management). Upravljanje finančnih virov za zagotavljanje ustreznih ciljev. Finančno upravljanje običajno vključuje stroškovno spremljanje in analize, nadzor nad razpoložljivimi sredstvi, oceno projektnih investicij in v nekaterih organizacijah tudi povrnitev stroškov.
- Proces **upravljanje delovne sile** (Workforce Management) priporoča načine za novačenje delovne sile ter kako obdržati in motivirati obstoječo delovno silo znotraj IT.

- Proces **upravljanje stalnosti storitve** (Service Continuity Management) se osredotoča na postopke in komponente potrebne za minimizacijo izpadov storitve z vseh vidikov, tudi s stališča obnovitve po katastrofi in popolnem izpadu ali izgubi podatkov ali infrastrukture.

Ti procesi definirajo in proizvajajo spremembe (nove verzije) s ciljem zmanjšanja stroškov in/ali izboljšanja storitev. *Revizija odobritve sprememb* je finalni pregled predlaganih sprememb. Po tem pregledu se začne nov cikel s procesi v kvadrantu sprememb.

Skupinski model

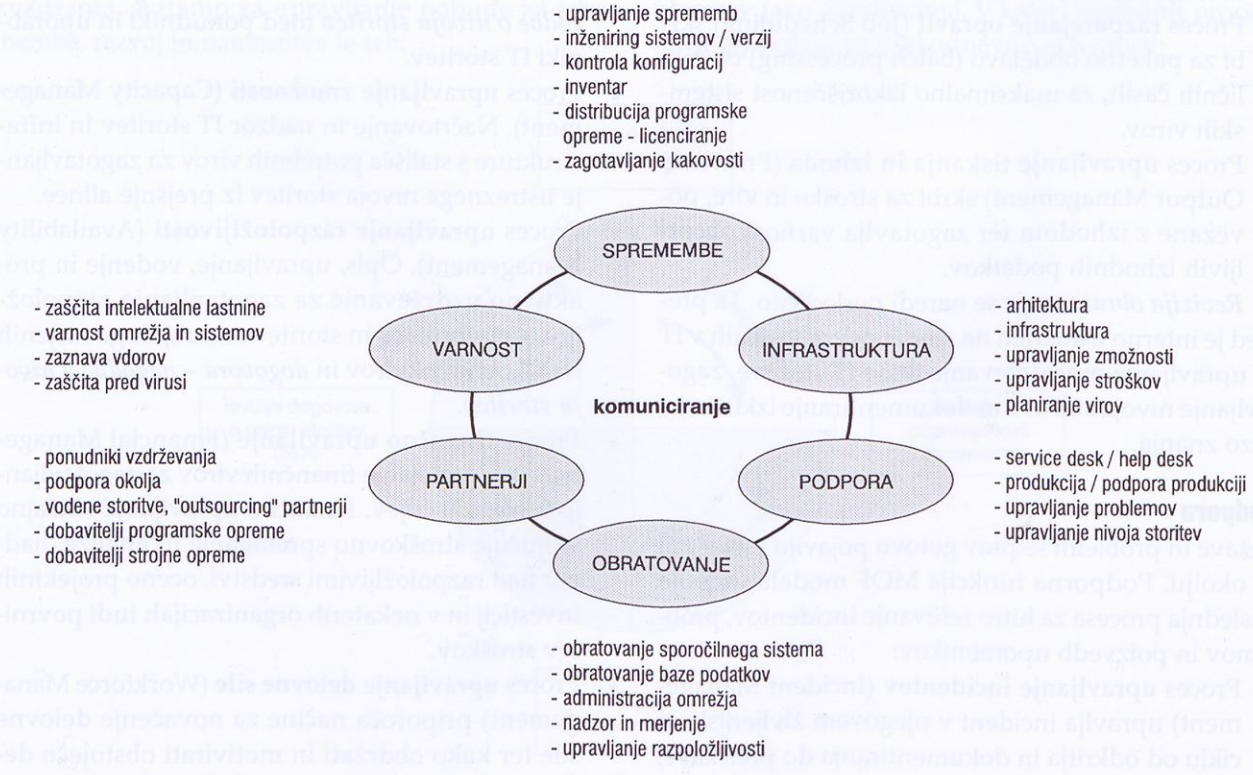
IT sistemi postajajo vse bolj zahtevni. Ravno tako so vedno bolj zahtevne aktivnosti in potrebno znanje za njihovo upravljanje in vodenje. Vse naloge, ki jih definirajo procesi, zahtevajo, da je skupina ljudi, ki jih izvaja, dobro organizirana in koordinirana. MOF skupinski model je skupek uporabnih navodil, ki poenostavljajo vidike vlog v skupini in pomagajo učinkovito organizirati ljudi. MOF skupinski model opisuje:

- najboljše izkušnje pri strukturiranju skupin in definicija posameznih vlog,
- ključne aktivnosti in zmožnosti posamezne vloge,
- velikost skupin za različne velikosti in tipe organizacij,
- katere vloge so lahko uspešno in učinkovito združene,
- principe in vodila, kako obratovati v razporejenem (distributed) okolju na Microsoftovi platformi,
- kako sta povezana MOF in MSF skupinski model.

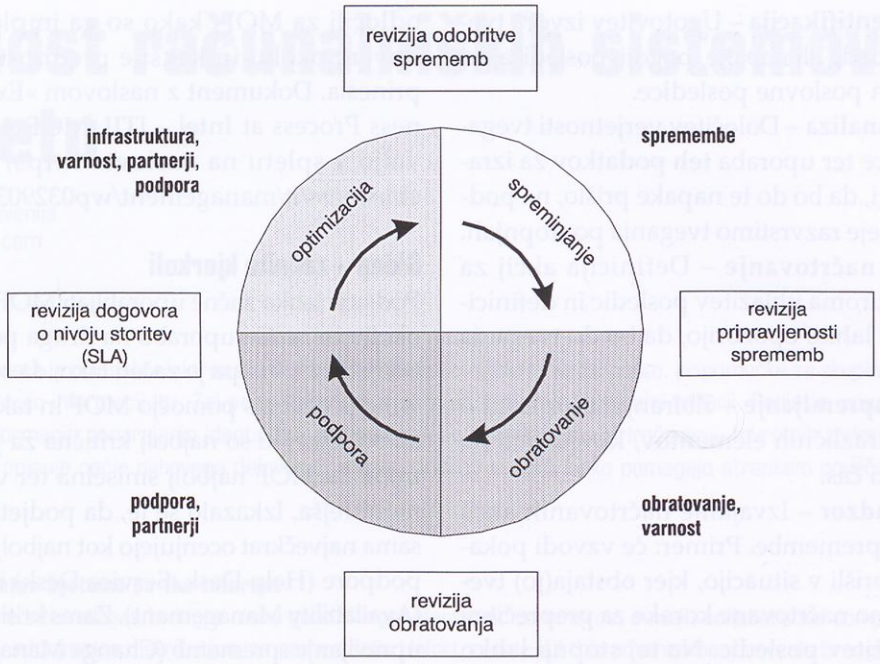
Skupinski model definira šest kategorij aktivnosti in procesov. Procesi znotraj vlog v skupinskem modelu so usmerjeni k istemu cilju – vsi ljudje znotraj ene vloge skupinskega modela imajo enake cilje. Vloge niso opisi delovnih mest in ne določajo organizacijske sheme podjetja ali oddelka. Število ljudi v posamezni vlogi je variabilno, lahko pa tudi ena oseba zaseda več vlog hkrati.

Na sliki 3 je prikazan diagram, ki kaže povezave med vlogami in funkcijami znotraj vlog.

Vloge skupinskega modela so tesno povezane s procesnimi kvadranti. Na sliki 4 vidimo, kakšna je koleracija med vlogami in procesi. V posameznem procesu lahko nastopa več vlog, hkrati pa lahko ista vloga nastopa pri različnih procesih.



Slika 3: **Skupinski model MOF**

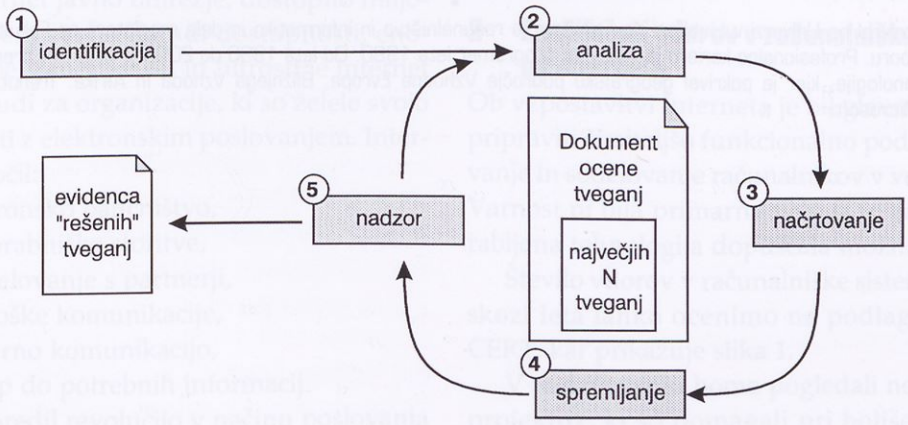


Slika 4: **Korelacija med procesi in vlogami**

Model tveganj

Model tveganj uporablja preverjene tehnike upravljanja s tveganji na problemih, ki jih IT osebje redno srečuje in rešuje. Obstaja veliko modelov, okvirjev in procesov za upravljanje s tveganji. Večina jih govori o načrtovanju negotove prihodnosti in MOF model tveganj ni nobena izjema. Kljub temu pa ponuja dodano vrednost skozi ključne principe, kot so terminologija (enaka skozi ves MOF pa tudi MSF okvir), strukturiran in ponovljiv proces petih korakov ter popolna integracija v celoten MOF in MSF.

Na sliki 5 vidimo korake procesa upravljanja s tveganji: identifikacija, analiza, načrtovanje, spremljanje in nadzor. Pomembno je razumeti, da gre vsako tveganje skozi vse stopnje vsaj enkrat, lahko pa tudi večkrat, kar se v praksi pogosto zgodi. Za vsako tveganje je definiran tudi časovni okvir, tako da se s stališča časa lahko v določenem trenutku v posamezni stopnji nahaja več tveganj hkrati. Takole pa so definirani koraki procesa:



Slika 5: **Proces upravljanja s tveganji**

- Prvi korak: **identifikacija** – Ugotovitev izvora tveganja, vrsta izpada ali napake, pogoji, posledica pri obratovanju in poslovne posledice.
- Drugi korak: **analiza** – Določitev verjetnosti tveganja in posledice ter uporaba teh podatkov za izračun verjetnosti, da bo do te napake prišlo, na podlagi česar kasneje razvrstimo tveganja po stopnjah.
- Tretji korak: **načrtovanje** – Definicija akcij za preprečitev oziroma ublažitev posledic in definicija vzvodov, ki lahko opozorijo, da bo do tveganja prišlo.
- Četrti korak: **spremljanje** – Zbiranje informacij o spreminjanju različnih elementov, ki vplivajo na tveganje, skozi čas.
- Peti korak: **nadzor** – Izvajanje načrtovanih akcij kot odziv na spremembe. Primer: če vzvodi pokažejo, da smo prišli v situacijo, kjer obstaja(jo) tveganja, izvedemo načrtovane korake za preprečitev oziroma ublažitev posledic. Na tej stopnji lahko tudi ugotovimo, da konkretnega tveganja ni več, kar pomeni, da ga izločimo iz nadaljnjega kroženja po ciklu.

Izkušnje

Veliko različno velikih podjetij že danes uporablja modele in okvire, kot so ITIL, MOF in MSF. Na spletu lahko najdete tudi precej dokumentov, ki opisujejo izkušnje podjetij pri vpeljavi. Prav tako obstaja kar nekaj podjetij (tudi v Sloveniji), ki se ukvarjajo s svetovanjem in pomočjo pri vpeljavi ITIL, MOF in MSF, in na katere se je zagotovo pametno obrniti ter izkoristiti njihovo znanje in izkušnje. Omenimo Intel, ki je pred kratkim objavil dokument o tem, zakaj so se odločili za MOF, kako so ga implementirali v njihovem okolju in kakšne prednosti jim je uporaba prinesla. Dokument z naslovom »Examining IT Business Process at Intel – ITIL/MOF Assessment« je na voljo v spletu na naslovu: http://www.intel.com/ebusiness/it/management/wp032903_sum.htm.

Sklep – začnite kjerkoli

Podjetje lahko začne uporabljati MOF kjerkoli v svojem okolju in razširi uporabo na druga področja in na celo podjetje. Dobro pa je začeti tako, da se opravi ocena celotnega okolja s pomočjo MOF in tako določi področja ali oddelke, ki so najbolj kritična za podjetje in bi bila uporaba MOF najbolj smiselna ter vrnitev investicije najhitrejša. Izkazalo se je, da podjetja in organizacije sama največkrat ocenjujejo kot najbolj kritična področja podpore (Help Desk, Service Desk) in razpoložljivosti (Availability Management). Zares kritični pa sta področji upravljanje sprememb (Change Management) in upravljanje izdaj (Release Management), kar se kaže tudi v nedavnih dogodkih in problemih z virusi, katerih večino bi kvalitetno upravljanje sprememb drastično zmanjšalo ali celo v celoti odpravilo.

Literatura

- ITIL – The Key to Managing IT Services – Best Practice for Service Support, OCG, 2002.
- ITIL – The Key to Managing IT Services – Best Practice for Service Delivery, OCG, 2002.
- Microsoft Operations Framework Essentials, Training Material MOC 1737, 2001.
- Ivor Macfarlane, Colin Rudd, IT Service Management, A companion to IT Infrastructure Library, itSMF, 2001.

Primož Karlin je diplomiral na Univerzi v Ljubljani na Fakulteti za računalništvo in informatiko in dela magisterij na Fakulteti za organizacijske vede Univerze v Mariboru. Profesionalno kariero je začel kot programer leta 1990. Od leta 1996 do 2003 je delal kot predavatelj in svetovalec za Compaq / HP tehnologije, kjer je pokrival geografsko področje Vzhodne Evrope, Bližnjega Vzhoda in Afrike. Trenutno je kot svetovalec zaposlen v podjetju Microsoft.

Varnost računalniških sistemov na internetu

Borut Žnidar, IBM Slovenija
borut.znidar@si.ibm.com

Povzetek

Eksplozivna rast interneta je prinesla elektronsko trgovino in bančništvo, elektronsko pošto, pripomočke za skupinsko delo, lažji dostop do materialov, distribucijo informacij itn. Žal pa ta napredek in varnosti ogrožajo kriminalni hekerji. Podjetja, posamezniki in država se bojijo zlorab, kraje informacij, ponarejanja identitete, spreminjanja dokumentov ipd. Prireševanju tovrstnih zadreg lahko pomagajo t.i. etični hekerji. Članek opisuje način njihovega delovanja, znanje, pristop in kako lahko pomagajo strankam povečati varnost pri delu z internetom.

Abstract

Security of the Computer Systems on the Internet

Explosive growth of the Internet has brought many good things: electronic commerce, e-mail, collaborative computing, easier access to reference material, information distribution, to name a few. Unfortunately, all this advancement reveals brought also the dark side: criminal hackers. Companies, private citizens and government would like to be part of this revolution, but there is always fear of misuse of information, identity, change of documents,... With this in mind we can call on ethical hackers for help. This paper describes the way ethical hackers work, their knowledge, approach and how they can help customers to improve security while working on Internet.

1 Uvod

Internet ali medmrežje je svetovni sistem računalniških omrežij – omrežje omrežij, v katerem lahko uporabniki na poljubnem računalniku dostopajo do informacij na drugem računalniku, če imajo pravico dostopa. Nastanek omrežja je omogočila ARPA (Advanced Research Projects Agency) in je bilo v začetku znano kot ARPANET. Osnovni namen je bil vzpostavitev omrežja med raziskovalnimi računalniki na različnih univerzah. Stranski učinek izbrane arhitekture je bil delovanje omrežja tudi v primeru izpada dela omrežja.

Danes je internet javno omrežje, dostopno miljonom ljudi po vsem svetu. Zaradi dostopnosti, enostavnosti uporabe, zanesljivosti in hitrosti je internet postal zanimiv tudi za organizacije, ki so želele svojo dejavnost razširiti z elektronskim poslovanjem. Internet jim je omogočil:

- izvajati elektronsko bančništvo,
- izboljšati uporabniške storitve,
- izboljšati sodelovanje s partnerji,
- zmanjšati stroške komunikacije,
- izboljšati interno komunikacijo,
- hitrejši dostop do potrebnih informacij.

Internet je naredil revolucijo v načinu poslovanja podjetij, na drugi strani pa je prinesel tveganje, ki je lahko usodno za poslovanje podjetij. Vdori v internetu lahko privedejo do izgube denarja, časa, izdelkov, ugleda, zaupnih informacij itn.

Vsi ti razlogi so zadosten pogoj za povečano zanimanje IT strokovnjakov in vodstev podjetij za načine varovanja računalniških sistemov v dobi internetnega poslovanja.

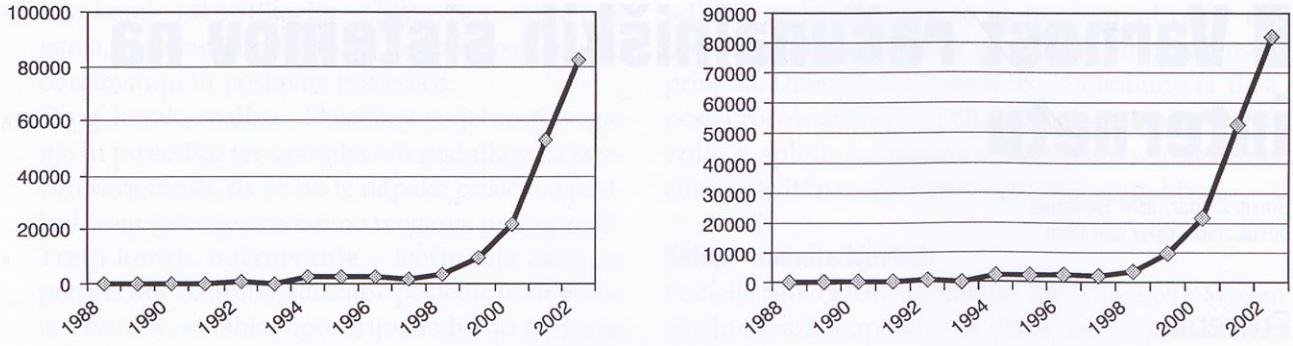
V nadaljevanju opisujemo razvoj napadov na internetu, sedanje stanje in najpogostejše načine napadov. Nadalje so opisani enostavnejši in bolj kompleksni načini zaščite.

2 Značilnosti vdorov v računalniške sisteme na internetu

Ob vzpostavitvi interneta je bil glavni namen le-tega pripraviti čimboljšo funkcionalno podlago za povezovanje in sodelovanje računalnikov v velikem omrežju. Varnost ni bila primarna naloga in zato je tudi uporabljena tehnologija dopuščala možnosti zlorabe.

Število vdorov v računalniške sisteme na internetu skozi leta lahko ocenimo na podlagi prijav centru CERT, kar prikazuje slika 1.

V nadaljevanju bomo pogledali nekaj institucij in projektov, ki so pomagali pri boljšem vpogledu v količino, obliko in namen vdorov na internetu, kakor tudi način zavarovanja pred njimi.



Slika 1: **Incidenti javljeni v CERT/CC [2]**

2.1 Koordinacijski center CERT

Koordinacijski center CERT (Computer Emergency Response Team) [1] je bil ustanovljen leta 1988 po pojavu internetnega črva Morris.

Namen CERT/CC je reagirati na varnostne težave na internetu, predstavljati centralno točko za prijavljanje odkritih varnostnih ranljivosti, služiti kot model pri vzpostavljanju za odzivanje na varnostne dogodke (incident response teams) in dvig zavesti o varnostnih problemih.

Od ustanovitve se je CERT/CC odzval na prek 50.000 varnostnih incidentov, ki so vplivali na stotisoče internetnih strani, delal je na več kot 1600 javljenih pomankljivosti/ranljivostih in izdal stotine priporočil in objav. Dodatno je pomagal pri vzpostavljanju osemdesetih drugih ekip za odzivanje na varnostne dogodke.

2.2 Eksperiment San Diego

Konec leta 1999 so v San Diego Supercomputer centru na internet priključili strežnik (Red Hat Linux v5.2) brez dodatnih varnostnih dodatkov ali nastavitev [5]. Strežnik ni bil v uporabi in njegova namestitev ni bila nikjer objavljena. Služil je le kot pasivna tarča za napadalce, na katerem so nato opazovali dogajanje:

- 8 ur po namestitvi:
  - poskus uporabe "Solaris RPC" ranljivosti – neuspešno;
- 21 dni po namestitvi:
  - 20 poskusov izrabe raznih ranljivosti, vključujočih POP, IMAP, telnet, RPC, mountd, ki pa so bili neuspešni, ker so bili narejeni za Red Hat 6.x;
- 40 dni po namestitvi:
  - uspešno izrabljena ranljivost POP serverja,
  - brisani nekateri sistemski logi,
  - instaliran rootkit in sniffer.

Ta poizkus je tako že pred leti pokazal, da je sistem že takoj, ko je priključen v internet, izpostavljen napadom, tudi če na njem sploh ni v uporabi noben servis. Razlika po štirih letih od poizkusa je le v tem, da je čas od priklopa do začetka napadov v povprečju bistveno krajši.

2.3 Projekt pregleda nad internetom

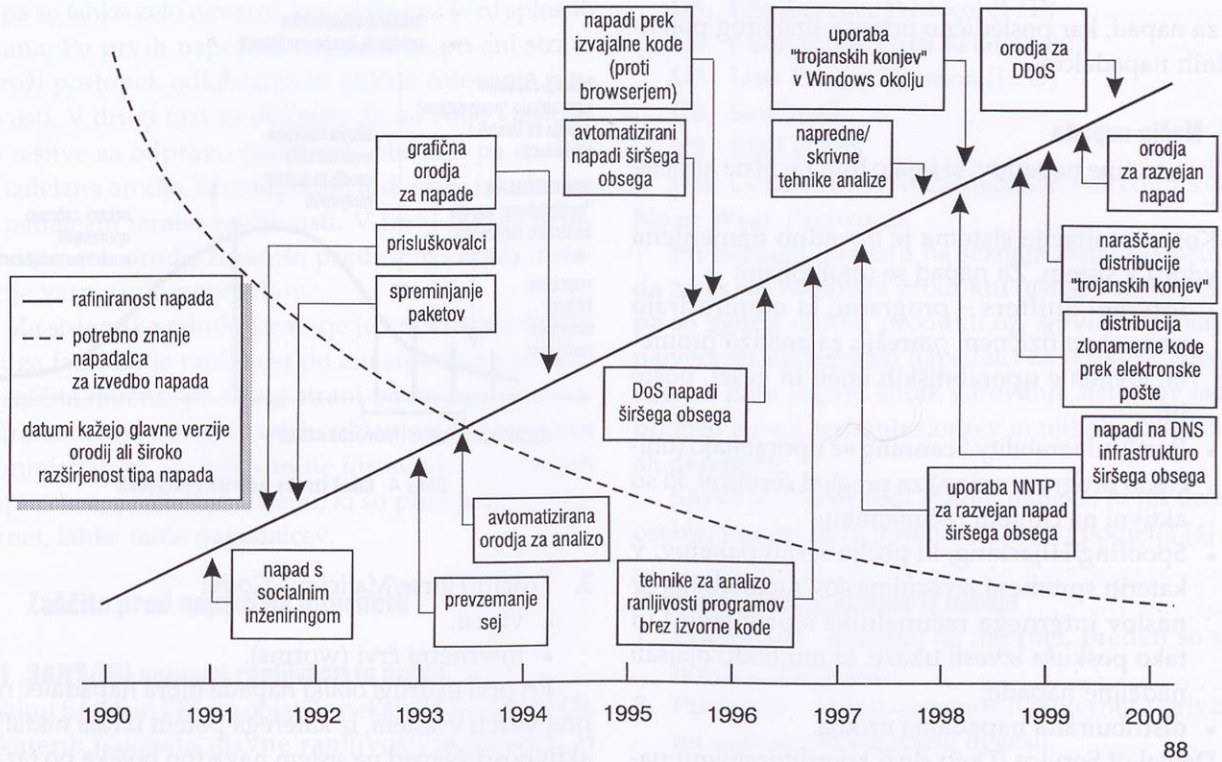
Projekt pregleda nad internetom (Internet Auditing Project) [6] poskuša gledati na varnost na internetu kot celoto, ne le kot na varnost posameznih računalnikov in omrežij. Projekt obravnava internet kot živ organizem, ne pa kot omrežje.

Projekt je leta 1999 začel Liraz Siri. Prvi varnostni pregled interneta je pokril 36 milijonov IP naslovov, kar je decembra 1998 pomenilo 85 % aktivnega adresnega prostora.

Preverjanje je trajalo dvajset dni in je bilo vzporedno izvajano iz Izraela, Mehike, Rusije, Japonske in Brazilije. Naslovnega prostora je bilo za 300 milijonov IP naslovov. Preverjenih je bilo osemnajst ranljivosti operacijskih sistemov Unix in v tem času so našli 730.000 ranljivosti na 450.000 računalniških sistemih. Projekt je opozoril na veliko ranljivost interneta in na številne sisteme, na katerih ni zagotovljena niti minimalna raven varnostne zaščite.

2.4 Inštitut SANS

SANS (System Administration, Networking and Security) Institute je bil ustanovljen leta 1989 kot raziskovalno-izobraževalna organizacija; več kot 156.000 var-



Slika 2: **Kompleksnost napadov glede na tehnično znanje napadalcev (po letih)**

nostnim strokovnjakom, nadzornikom (auditor), sistemskim in mrežnim administratorjem omogoča izmenjavo informacij in pomaga pri reševanju težav in izzivov, s katerimi se srečujejo. Njegovo jedro so varnostni strokovnjaki v državnih agencijah, organizacijah in univerzah po vsem svetu, ki investirajo stotine ur vsako leto v razvoj in izobraževanje za informacijsko varnost.

3 Napadalci in načini napadov

3.1 Kdo je "hacker" in kdo "cracker"

Heker (angl. hacker) je izraz, s katerim nekateri označujejo "spretnega programerja", drugi pa "nekoga, ki poskuša vdreti v računalniški sistem".

1. Eric Raymond, avtor *The New Hacker's Dictionary*, je definiral hekerja kot spretnega programerja. Dober "hack" je spretna rešitev programerskega problema in "hacking" je oznaka tega dela.
   Raymond ne priporoča uporabe tega izraza za tiste, ki poskušajo vdreti v sistem drugih ali na drug način uporabljajo znanje programiranja ali drugo strokovno znanje za zlonamerno delovanje. Za te predlaga izraz "cracker".
2. Novinarji pretežno uporabljajo izraz heker za nekoga, ki poskuša vdreti v računalniški sistem. Navadno je to izkušen programer ali inženir z dovolj tehničnega znanja, da razume šibke točke v varnostem sistemu.

Cracker je oseba, ki vdre v računalniški sistem nekoga drugega, ki je običajno priključen v omrežje, obide geslo ali licence računalniškega programa ali na drug način nalašč prebije računalnikovo zaščito. Cracker dela to za zaslužek, zlonamerno, za kakšen nesebičen namen ali načelo, ali zgolj zato, ker se je pojavila priložnost. Nekateri vdori so bili opravljeni navidezno, da bi pokazali slabosti v varnostnem sistemu.

Za napadalce na računalniške sisteme prek interneta je značilno, da:

- z napadi gradijo tehnično znanje in izkušnje,
- pridobivajo vpliv z avtomatizacijo,
- raziskujejo medmrežne povezave in enostavno gibanje skozi infrastrukturo,
- postajajo bolj izkušeni pri zakrivanju svojega delovanja.

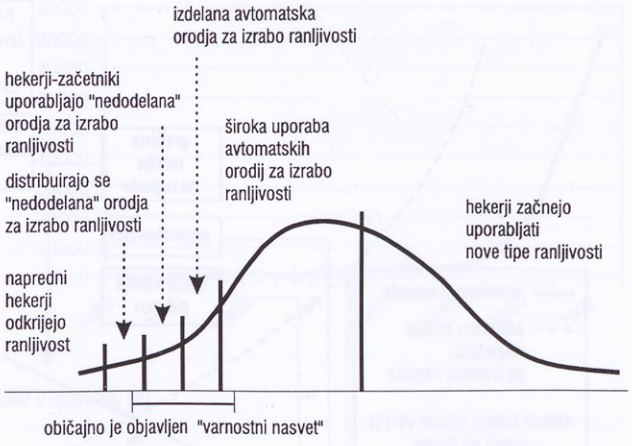
Kot nam kaže slika 2, se kompleksnost napadov povečuje, obenem pa se zmanjšuje tehnično znanje napadalcev. To je posledica vedno bolj dodelanih oro-

dij za napad, kar posledično prinese širši krog potencialnih napadalcev.

3.2 Način napada

Ločimo tri tipe napadov, ki imajo tudi različne končne cilje:

1. Kompromitacija sistema je navadno namenjena vdoru v sistem. Za napad se uporabljajo:
   - Internet Sniffers – programi, ki monitorirajo promet na fizičnem omrežju za analizo prometa, lovljenje uporabniških imen in gesel, pošte itn.;
   - Port/Vulnerability Scanning se uporabljajo (običajno program nmap) za pregled servisov, ki so aktivni na ciljnem računalniku;
   - Spoofing/Hijacking, ki pošlje serijo paketov, v katerih spremeni izvorni naslov računalnika (v naslov internega računalnika s privilegiji) in tako poskuša izvesti ukaze, ki mu bodo olajšali nadaljne napade;
   - distribuirana napadalna orodja.
2. Denial of Service (DoS) služi koordiniranemu napadu na sisteme internet z namenom, da jih zruši:
   - enostavni DoS – namen napadalca je napraviti ciljni računalnik nedosegljiv uporabnikom;
   - distribuirani Denial of Service (DDoS) – pri tem načinu napada uporabimo isto tehnologijo kot v DoS napadu, le da je napad izveden iz več (že napadenih in zavzetih) računalnikov hkrati.



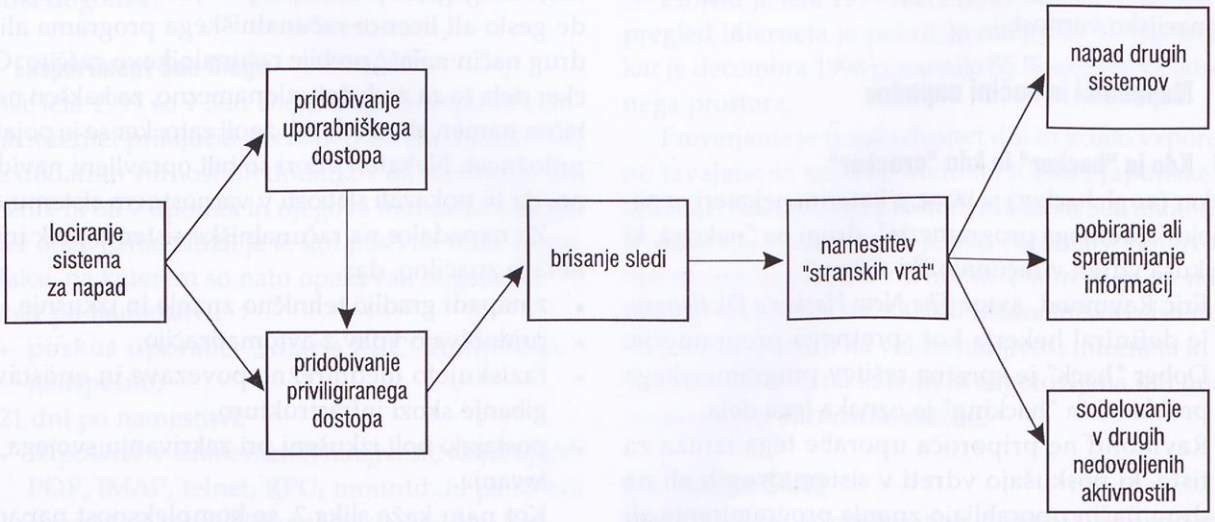
Slika 4: **Cikel izrabe odkrite ranljivosti**

3. Trojan Horse/Malicious Code:
   - virusi,
   - internetni črvi (worms).

Pri prvi in drugi obliki napada mora napadalec najprej vdreti v sistem, iz katerega potem izvaja nadaljne aktivnosti. Napad na sistem navadno poteka po fazah, ki jih prikazuje slika 3.

Ranljivosti, ki jih napadalci izrabljajo, pokažejo določene zakonitosti uporabe, ki jih kaže slika 4.

V prvi fazi izkušeni napadalci odkrijejo ranljivost in tudi izdelajo prva orodja za njihovo izkoriščanje, ki pa so običajno precej zahtevna za uporabo. V tej fazi je število možnih napadalcev relativno majhno, napa-



Slika 3: **Običajen potek napada.**

di pa so lahko zelo nevarni, ker ranljivost še ni splošno znana. Po prvih uspešnih napadih se po eni strani sproži postopek odkrivanja in zaščite reševanja ranljivosti. V drugi fazi so običajno že na voljo varnostne rešitve za odpravo ranljivosti, obenem pa so tudi že izdelana orodja, ki omogočajo tudi manj izkušenim napadalcem izrabo ranljivosti. V tretji fazi se učinkovitost teh orodij zmanjša predvsem zaradi instalacije varnostnih popravkov.

Za sistemske administratorje je kritična predvsem druga faza, ko je ranljivost po eni strani že znana in je zaščita možna, po drugi strani pa imamo avtomatizirana orodja za njihovo izkoriščanje. Če v tem času administratorji »zaspijo« in ne instalirajo varnostnih popravkov, postanejo sistemi, ki so priključeni na internet, lahke tarče napadalcev.

4 Zaščita pred napadi na internetu

4.1 SANS/FBI seznami ranljivosti in napak

Inštitut SANS in FBI sta objavila nekaj dokumentov [3], v katerih navajata glavne ranljivosti in napake. Ti seznami ranljivosti in napak so koristna informacija, saj večina uspešnih napadov na računalniške sisteme na internetu temelji na ranljivostih iz spodnjih seznamov.

Glavne ranljivosti Windows sistemov

W1 Internet Information Services (IIS)

W2 Microsoft Data Access Components (MDAC) – Remote Data Services

W3 Microsoft SQL Server

W4 NETBIOS – Unprotected Windows Networking Shares

W5 Anonymous Logon – Null Session

W6 LAN Manager Authentication – weak LM Hashing

W7 General Windows Authentication – Accounts with No or Weak Passwords

W8 Internet Explorer

W9 Remote Registry Access

W10 Windows Scripting Host

Glavne ranljivosti Unix sistemov

U1 Remote Procedure Call (RPC)

U2 Apache Web Server

U3 Secure Shell (SSH)

U4 Simple Network Management Protocol (SNMP)

U5 File Transfer Protocol (FTP)

U6 r-Services – Trust Relationship

U7 Line Printer Daemon (LPD)

U8 Sendmail

U9 BIND/DNS

U10 General Unix Authentication – Accounts with No or Weak Passwords

Pri bežnem pogledu na seznam dobimo občutek, da zares pri nobenem produktu nismo varni. Vseeno pa so zgoraj našteti produkti oz. servisi tisti, katere največkrat uporabljajo napadalci za poskuse vdora v sistem. Zato je prvi korak varovanja sistemov lahko pregled zgoraj naštetih storitev in njihova izključitev ali okrepitev.

SANS je objavil tudi glavne napake, ki jih dela IT osebje, končni uporabniki in vodstvo podjetja [4] .

Glavne varnostne napake IT osebja

1. Priključitev sistemov na internet, preden so varnostno okrepljeni.
2. Priključitev testnih sistemov na internet s privzetimi uporabniškimi imeni in gesli.
3. Neupešna posodobitev sistemov po odkritih varnostnih luknjah.
4. Uporaba telneta in drugih nekriptiranih protokolov za upravljanje sistemov, routerjev, požarnih pregrad in PKI.
5. Dodeljevanje in sprememba uporabniških gesel prek telefona brez avtorizacije prosilca.
6. Neuspešno upravljanje in testiranje varnostnih kopij.
7. Delovanje nepotrebnih servisov, npr. ftpd, telnetd, finger, rpc, mail, r-servisov idr.
8. Implementacija požarne pregrade s pravili, ki ne zaustavijo zlonamernega in nevarnega prometa.
9. Neuspešna vzpostavitev ali posodobitev sistema za odkrivanje virusov.
10. Neuspešno izobraževanje uporabnikov o potrebnih akcijah v primeru varnostnih problemov.

Glavne napake vodstva podjetij

1. Dodelitev neusposobljenih ljudi na varnostne funkcije, brez možnosti za usposabljanje za obvladovanje varnosti.
2. Nerazumevanje razmerja med varnostjo informacij in poslovnimi problemi. Razumejo le fizično varnost in ne vidijo posledic slabe varnosti informacij.

3. Nezmožnost izvajanja operativnih nalog varnosti: stalna kontrola, da so sistemi na zadnjem nivoju popravkov.
4. Zanašanje predvsem na požarno pregrado.
5. Nezmožnost ugotoviti, koliko so vredne informacije in sloves podjetja.
6. Odobritev zakasnelih, kratkoročnih popravkov, zato se problem hitro povrne.
7. Upanje, da bo problem izginil, če ga bodo ignorirali.

Glavne varnostne napake končnih uporabnikov

1. Neuspešna instalacija antivirusnih programov, njihovo redno vzdrževanje (popravkov in virusnih definicij) ter njihova implementacija na vse datoteke.
2. Odpiranje prilog elektronske pošte brez preverjanja pošiljatelja in vsebine ali izvajanje iger in ohranjevalnikov zaslona iz nepreverjenih virov.
3. Neuspešna instalacija varnostnih popravkov, predvsem za Microsoft Office, Microsoft Internet Explorer in Netscape.
4. Ni izdelave varnostnih kopij oz. njenega preverjanja.
5. Uporaba modema ob hkratni priključenosti na lokalno omrežje.

Ti trije seznami pomenijo predvsem dobro izhodiščno točko pri odpravljanju problema internetnih napadov. Predstavljajo najpogostejše napake in če jih pričnemo upoštevati, bomo krepko zmanjšali možnost napadov.

5 Etični heking

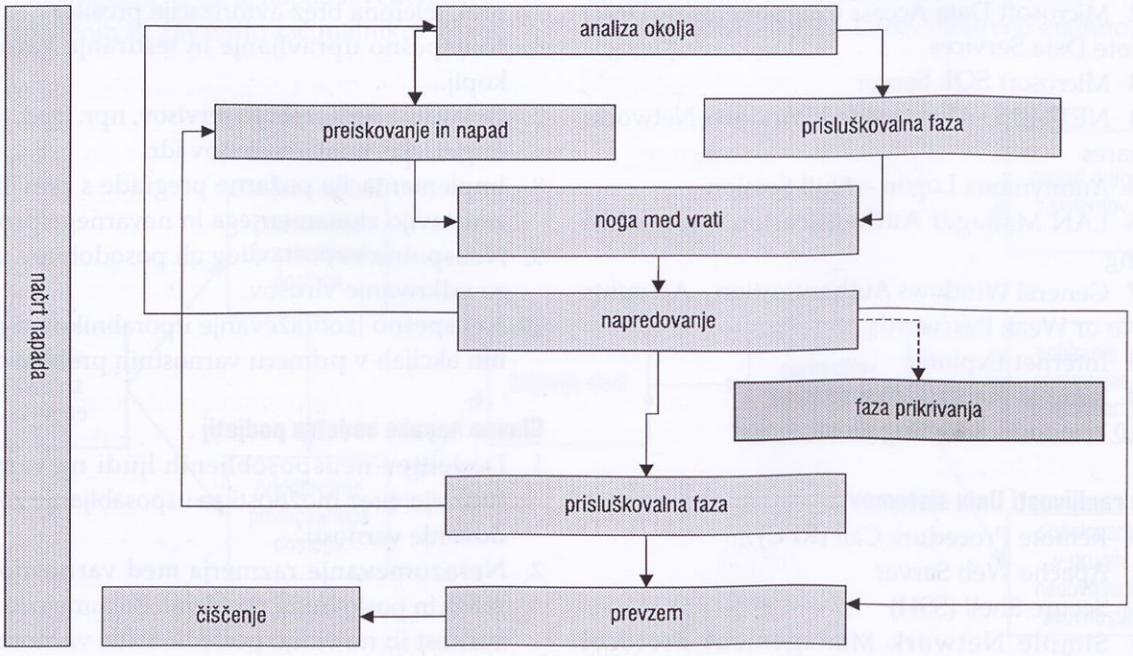
5.1 Kdo je „etični heker“

Etični heker je računalniški in mrežni strokovnjak, ki izvaja napad na računalniški sistem na podlagi zahteve lastnika tega sistema. Pri tem išče pomankljivosti, ki bi jih zlonamerni heker lahko izkoristil. Za preverjanje varnosti sistema uporablja iste metode kot crackerji, vendar ugotovitve ne izkoristi, temveč jo objavi v poročilu.

Etični heking je poznan tudi pod imenom test vdora (penetration testing, intrusion testing) ali "red teaming". Etičnega hekerja včasih imenujejo tudi "white hat"; izraz prihaja iz starih vesternov, kjer so"dobri fantje" nosili bele klobuke, "slabi fantje" pa črne.

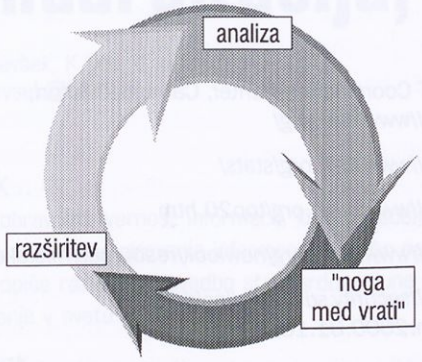
5.2 Metodologija

Metodologija, ki jo uporabljajo etični hekerji, je podobna napadom crackerjev in je sestavljena iz treh de-



Slika 5: **Diagram napada**

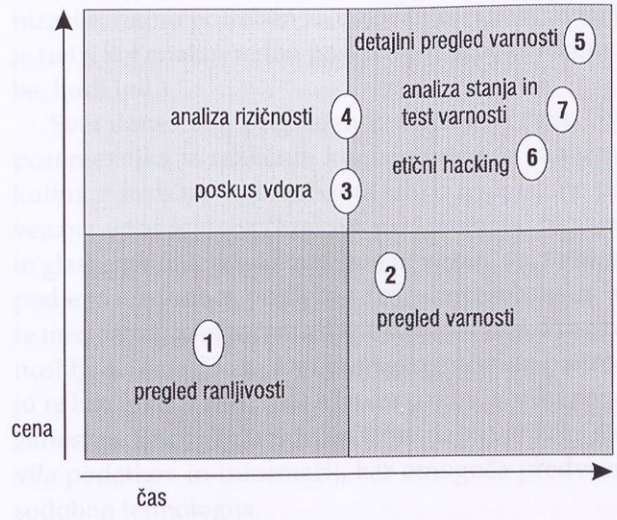
lov: analize, vdora, stopnjevanja. Ta pristop se ponavlja ciklično in predstavlja napadalni cikel:



- Analiza okolja (Reconnaissance):
  - pridobivanje informacij,
  - iskanje ranljivosti.
- Noga med vrati:
  - izkoristi ranljivost,
  - pridobivanje dostopa.
- Stopnjevanje:
  - povečanje privilegijev (pridobivanje administracijskih privilegijev).

Razdelani diagram napada prikazuje Slika 5:

1. Analiza okolja (Reconnaissance) – nabiranje informacij o ciljnem sistemu ali omrežju.



Slika 6: **Vrste preverjanja varnosti interneta**

2. Preiskovanje in napad (Probe and attack) – preiskovanje slabosti sistema in priprava/izbira orodij za napad.
3. Noga med vrati (Gaining a toehold) – izraba varnostnih slabosti za pridobivanje dostopa v sistem.
4. Napredovanje (Advancement) – napredovanje iz nepriviligiranega v priviligiranega uporabnika.
5. Faza prikrivanja (Stealth phase) – skrivanje sledov.
6. Prisluškovalna faza (Listening phase) – vzpostavi prisluškovanje z uporabo snifferjev.
7. Prevzem (Takeover) – razširitev kontrole iz enega sistema na druge sisteme v omrežju.
8. Čiščenje (Cleanup).

Servis etičnega hekinga navadno ne vključuje faze prikrivanja, razen če stranka to zahteva.

5.3 Open-Source Security Testing Methodology

ISECOM [8] (Institute for Security and Open Methodologies) je organizacija, ki je pripravila predlog metodologije OSSTMM [9], [10] z natančno razdelanim načinom izvedbe varnostnega testiranja. Glede na vloženo količino časa in denarja razlikujejo različne vrste testiranja, od najenostavnejšega pregledovanja ranljivosti, prek etičnega hekinga do celotnega varnostnega pregleda, kar prikazuje slika 6.

Njihov varnostni načrt obsega pregled šestih med seboj povezanih področij, ki vsebujejo elemente drugih področij in pokažejo pravo sliko testiranja šele kot celota:

1. informacijska varnost (information security),
2. procesna varnost (process security),
3. varnost internetne tehnologije (Internet technology security),
4. komunikacijska varnost (communications security),
5. varnost "wireless" tehnologije (wireless security),
6. fizična varnost (physical security).

5.4 Izvajanje storitve etičnega hekinga

IBM varnostni servis [11] »internet varnostni pregled« [12] simulira poskus vdora v naročnikov IT sistem v kontroliranem in za naročnika varnem načinu. Storitev je poglobljena in obsežna, poleg vidika vdora pa pokriva še konfiguracijo in upravljanje sistemov, s čimer celovito obravnava vse dejavnike, ki bi lahko negativno vplivali na internetno varnost stranke v prihodnosti.

Storitev daje kot rezultat celovit pregled nad varnostnim stanjem internetnega dostopa na tehničnem

in upravljalskem nivoju. Pregled s tehnološkega vidika vsebuje testiranje različnih načinov vdorov in analizo konfiguracije ter s tem daje pregled nad stanjem in pove šibke točke varnosti internetnega dostopa do virov podjetja. Upravljalski vidik pregleda se opravi s pogovori z administratorji in vodilnimi v podjetju o varnostni dokumentaciji, procesih in standardih. Oba pregleda skupaj dajeta podroben vpogled v stanje varnosti internetnega dostopa in pripravljenost na morebitne poskuse vdora nepooblaščenih tretjih oseb z interneta.

6 Sklep

Internet je nova poslovna paradigma, ki se razvija in ponuja številne možnosti za ljudi z vizijo in pogumom. Učinkovito konkuriranje v globalni ekonomiji zahteva od podjetij prilagajanje povečanje stopnje odprtosti in dostopnosti. Vendar morajo podjetja, ki poskušajo prodreti na novi obetajoči trg, ki ga ponuja internet, določiti in izvesti močne varnostne postopke, tako za povečanje svojih informacijskih sistemov, kakor tudi za ohranjanje zaupanja strank.

Internet je bil razvit za zagotavljanje dinamičnih, prilagodljivih in odprtih komunikacij med več različnimi sistemi. Zaradi svoje odprte zasnove sam po sebi ne more zagotavljati zaščite vključenih informacijskih sistemov.

Varnost informacijskih sistemov postaja z uporabo interneta in e-poslovanja vse pomembnejša in zaradi vključevanja osnovnih poslovnih dejavnostni v internetni način poslovanja tudi vse bolj izpostavljena. Zato bo še treba veliko pozornosti namenjati zagotavljanju in vzdrževanju varnosti IT sistemov na internetu.

7 Viri

[1] CERT Coordination Center, Carnegie Mellon, *http://www.cert.org/*

[2] *http://www.cert.org/stats/*

[3] *http://www.sans.org/top20.htm*

[4] *http://www.sans.org/newlook/resources/mistakes.php*

[5] *http://security.sdsc.edu/incidents/worm.2000.01.18.shtml*

[6] *http://www.viacorp.com/auditing.html*

[7] *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html*

[8] ISECOM – Institute for Security and Open Methodologies, *http://www.isecom.org/*

[9] OSSTMM - Open Source Security Testing Methodology Manual, *http://www.osstmm.org/*

[10] Herzog, Pete: OSSTMM 2.1. - Open-Source Security Testing Methodology Manual, 2003, *http://www.isecom.ca/mirror/osstmm.en.2.1.pdf*

[11] *http://www-3.ibm.com/security/index.shtml*

[12] *http://www-1.ibm.com/services/security/-intrspec.html*

Borut Žnidar zadnjih šest let del v IBM Slovenija, kjer dela na področjih varnosti, Unix in Linux operacijskih sistemov ter velikih strežnikov za slovenske stranke in tudi pri večjih projektih v regiji. Pred tem je osem let delal na pripravi, razvoju, implementaciji in vzdrževanju sistema za laboratorije v zdravstvu.

Informacijska varnost: standardizacija, da ali ne?

Rado Ključevšek, K.Sec, d. o. o.
rado.kljucevsek@ksec.si

Izvleček

Prispevek obravnava varnost informacij, ki jo opredeljuje kot poslovni problem. Pri poslovanju iščemo razširjene in priznane rešitve problemov, v primeru varovanja informacij se lahko naslonimo na standarde, konkretno na standarda ISO/IEC 17799 in BS 7799-2. Prispevek opiše razloge za uvedbo standardov, njune dobre strani, zgodovinsko ozadje in potrebe po njunem nastanku. Prikazano je njuno uvajanje v svetu in Sloveniji.

Abstract

Information Security: standardization, yes or no?

This article discurses information security which is shown as a business problem. In business we look for ubiquitous and recognized problem solutions and in the case of information security we can make use of standards in particular of the standards ISO/IEC 17799 and BS 7799-2. We give reasons for the implementation of the standards, their benefits when implemented as well as their historical background and the needs for their emergence. We show the situation regarding the implementation of the standards in the world and in Slovenia.

Uvod

Živimo v družbi znanja, kjer je le-to manifestirano v različnih pojavnih oblikah, med drugim tudi informacij, ki so gibalo razvoja v akademskoraziskovalnih institucijah in vir konkurenčnih prednosti v gospodarstvu. Vse organizacije svoje delovanje urejajo z informacijami, ki so popolnoma enakovredno poslovno sredstvo. Drugi viri so bolj ali manj enostavno dostopni.

Informacija je danes enakovreden vir vsake organizacije, nujno potreben za delovanje; obravnavati jo je treba kot enakovreden poslovni vir (kot npr. zgradbe, ljudi ipd.).

Svet danes bolj prepleten kot kdajkoli prej. Dva posameznika iz različnih koncev sveta, iz različnih kultur, z različno izobrazbo sta lahko neprestano povezana – kar je največkrat res pri izmenjavi filmskih in glasbenih datotek. Danes smo povezani vsi z vsemi; podjetja med seboj, podjetja s fizičnimi osebami in ljudje med seboj. Svet je manjši kot kdajkoli prej. Povezanost ljudi še na precej manjšem geografskem področju ni bila nikdar tako velika kakor danes. Velika povezanost pa neizogibno prinaša izmenjavo velikega števila podatkov in informacij, kar omogoča predvsem sodobna tehnologija.

K današnjemu pomenu informacij je precej pripomogla ravno sodobna tehnologija, ki omogoča zbiranje, shranjevanje in obdelavo velikega števila informacij. Seveda so vse sposobnosti sodobne tehnologije neuporabne, če nimajo predmeta obdelave, t. j. informacije. Danes podjetja in druge organizacije lahko pridejo do osupljivo točnih sklepov o željah in namerah državljanov/potrošnikov in z veliko zanesljivostjo napovedujejo prihodnje dogodke. Vsa ta količina informacij, zbrana v različnih bazah komercialnih in državnih ustanov, pa kar kliče po zlorabi. Možnosti zlorabe se povečujejo z naraščanjem števila koristnih informacij, enostavnostjo zlorabe in koristjo, ki jo tako dejanje prinaša. Vse to zahteva ukrepe zaščite informacij v lasti fizičnih in pravnih oseb.

Kljub visoki tehnologiji v podjetjih in zasebnem življenju se ne smemo pustiti zavesti pojmovanju, da je informacijska varnost predmet zgolj tehničnih rešitev. Informacije imajo namreč različne pojavne oblike; lahko so shranjene in posredovane v elektronski obliki, na papirju, lahko so shranjene v glavah ljudi in posredovane ustno. Prav vse oblike shranjevanja in posredovanja dopuščajo številne zlorabe. Resda so

možnosti zlorab pri neelektronskih oblikah enake kakor v preteklosti, vendar iz naštetih razlogov informacija še nikdar ni imela tako visoke vrednosti, kot jo ima danes.

Kaj je informacijska varnost?

Predmet informacijske varnosti je informacija v vseh svojih pojavnih oblikah. Varovanje informacij pomeni ohranjanje njene:

a) zaupnosti: informacija mora biti dostopna samo tistim osebam, ki so do tega upravičene in za to pooblaščene;
b) celovitosti: informacija mora biti točna, popolna in verodostojna;
c) razpoložljivosti: informacija in vsi z njo povezani viri morajo biti pooblaščenim osebam na voljo, kadarkoli želijo to svojo pravico udejaniti.

Praktiki varovanja informacij so prevečkrat tudi nosilci nalog informatike in svojo nalogo zato dojemajo preozko. Varovanje informacij pojmujejo kot tehnološki problem, problem zgolj informatike in informatikov. Vendar zagotavljanje varnosti informacij ni zgolj predmet postavitve požarnega zidu, uvedbe nujne uporabe gesel ali rezervnih kopij. Je že res, da je velika večina informacij v elektronski obliki, vendar so mnogokrat tudi te informacije predmet nič kaj elektronskih groženj – poplave, požari, tatvine dlančnikov in prenosnih računalnikov, vdorov v zgradbe in poslovne prostore in na koncu, vendar ne najmanj pomembno, človeškega faktorja – pozabljivosti ali neprevidnosti. Poleg tega je še vedno ne-zanemarljiva količina informacij shranjenih in posredovanih v neelektronskih oblikah.

Področje zagotavljanja varnosti informacij je torej izredno široko in zahteva celovit pristop. Problema varnosti informacij se zaradi vseh njenih pojavnih oblik ne da rešiti samo s tehničnimi napravami, ampak jih je praktično vedno treba kombinirati z drugimi ukrepi, postopki, standardi in politikami.

ISO 17799/BS 7799-2 in drugi varnostni standardi in priporočila

Varovanja informacij se lahko lotimo različno. Danes je upravljavcem varovanja informacij na voljo več standardov, dobrih praks, procedur, politik in metodologij. Nekatere so namenjene vsem organizacijam (na primer standarda ISO/IEC 17799, BS 7799-2, priporočila GASSP, OECD Guidelines – navodila za varnost informacijskih sistemov in mrež), druge so bolj specializirane, na primer za produkte (Common Criteria/ISO 15408), za informacijsko tehnologijo (GMITS/ISO 13335, metoda COBIT) in podobno.

Med vsemi referenčnimi sistemi je najbolj celovit in v svetu najbolj priznan standard ISO 17799/BS 7799-2. Njegova uporaba je neodvisna od pojavne oblike informacije. Naj si bo to pisna, elektronska ali ustna oblika, informacija, ko je spoznana kot vredna varovanja, je lahko v okviru sistema varovanja. Začetek standarda sega v zgodnja devetdeseta leta prejšnjega stoletja, leta 1993 pa je britanski DTI (Department of Trade and Industry) izdal Code of Practice, primere najboljše prakse s tega področja. Leta 1995 je bila izdana prva verzija standarda BS 7799. Takrat je BSI (British Standards Institute) izdal standard BS 7799, ki pomeni začetek današnjega prvega dela standarda. Prvi del standarda – kodeks – je bil nato izdan v popravljeni verziji še leta 1999 in 2000 kot ISO 17799 standard. Drugi del standarda BS 7799 – specifikacija – je bil prvič izdan leta 1998, nato pa še leta 1999 in leta 2002, obakrat v posodobljenih različicicah.

Standard BS 7799 je sestavljen iz dveh delov; prvi predstavlja najboljšo prakso pri izpolnjevanju zahtev po informacijski varnosti in je v praksi uporaben predvsem pri iskanju varnostnih rešitev in podrobnejši razlagi drugega dela standarda. Drugi del je specifikacija, zbirka lastnosti, ki jim mora sistem varovanja informacij ustrezati, če želi biti organizacija skladna s standardom in se po njem certificirati ter tako izkazovati sposobnost varovanja svojih informacij ininformacij njenih partnerjev. Drugi del BS 7799 standarda je trenutno v postopku mednarodnega priznanja institucije ISO.

Prvi del standarda nam torej odgovarja na vprašanje, kako NAJ BI delovala organizacija varovanja informacij, medtem ko drugi del predpisuje, kako MORA delovati takšna organizacija.

Glavni pomen ISO 17799/BS 7799-2 standarda je predvsem v njegovem drugem delu. Čeprav ima standard jasno definiranih 10 poglavij, 36 ciljev in 127 nadzorstev, za uporabnika niso vsi zavezujoči. Kar standard od uporabnika zahteva, je izvedba smiselnih korakov vzpostavitve sistema varovanja informacij. Resda 127 nadzorstev predvideva najboljšo poznano izvedbo določenih varnostnih varoval, vendar vsa niso potrebna vsem organizacijam. Standard poskuša biti z določenimi predpisanimi koraki kar se da gospo-

daren. Tako zahteva od vsakega uporabnika analizo tveganj kot temelja uvedbe sistema varovanja informacij. Šele ko poznamo tveganja naših informacijskih virov, lahko sprejemamo odgovorne in utemeljene odločitve. Tako izberemo samo tista nadzorstva, ki so odgovor na dejanska tveganja za našo organizacijo. Uvedba drugih bi bila ali nesmiselna ali neekonomična. Ravno na tej točki se standard BS 7799 razlikuje od drugih sistemov varovanja informacij – ne predvideva določenih ukrepov pred dejanskim poznavanjem tveganj.

Standard ISO 17799/BS 7799-2 je upravljavski standard. Od uporabnikov zahteva manedžerske/upravljavske odločitve. Vsaka organizacija izbere nivo in obliko varnosti, ki ustreza njenim (poslovnim) ciljem. Torej zasleduje izbrano razmerje strošek/učinek. Od organizacije zahteva predvsem poznavanje tveganj in na tej podlagi sprejemanje odločitev. Če je zmanjševanje ali prenašanje tveganj predrago in s tem neupravičeno (neprimerno razmerje količnika strošek/učinek), mora organizacija to navesti v načrtu protiukrepov, kar zadostuje zahtevam standarda. Kot tak je standard ISO 17799/BS 7799-2 kar se da življenjski.

Standard ISO 17799/BS 7799-2 je procesno orientiran. Temelji na procesni ureditvi poslovanja, kot jo poznamo iz ostalih razširjenih standardov – ISO 9000, 14000, OHSAS 18000. Informacija oz. informacijski vir kot predmet varovanja je opredeljen tudi v že omenjenih standardih kot vhodni, izhodni ali operativni vir procesa. Ta lastnost standarda ISO 17799/BS 7799-2 ni naključna. Ena glavnih namer standarda je njegova življenjskost in uporabnost. Tako ne sme revolucionarno posegati v obstoječe organizacijske strukture delovanja, temveč se jim mora čimbolj prilagajati, se z njimi spojiti in uporabljati obstoječo organizacijsko infrastrukturo za svoje delovanje.

Življenjskost standarda je poleg procesne razvidna tudi iz njegove druge temeljne usmeritve, ki sledi principom Demingovega kroga PDCA (Plan – Do – Check – Act), torej stalnega izboljševanja. Praktiki, predvsem v Sloveniji, še prepogosto govorijo o varnostnih politikah za urejanje varovanja informacij. Varnostna politika je le del sistema varovanja informacij. Ko politika zaživi in vstopi v cikel neprestanega izboljševanja, lahko govorimo o sistemu kot naslednji razvojni fazi varovanja informacij.

Za ilustracijo, ki naj bi pokazala splošnost in celovito pokritost, podajamo še pregled področij varovanja informacij, ki jih pokriva standard ISO 17799/BS 7799-2:

- politika varovanja,
- organiziranost varovanja,
- razvrstitev in nadzor informacijskih sredstev,
- varovanje v zvezi z osebjem,
- fizično in okolno varovanje,
- upravljanje s komunikacijami in obratovanjem,
- obvladovanje dostopa,
- razvijanje in vzdrževanje sistema,
- zagotavljanje neprekinjenega poslovanja,
- usklajenost z lokalno zakonodajo.

Stanje v svetu in v Sloveniji

Zavedanje o pomembnosti varovanja informacij v zadnjih letih tako v svetu kot v Sloveniji močno narašča. Temu primerna je tudi razširjenost števila prejemnikov certifikata BS 7799. Tudi njihovo število močno narašča. Danes je vseh imetnikov certifikata približno 400, pred dobrim letom jih je bilo okrog 150. Standard je najbolj razširjen na Japonskem in v Veliki Britaniji. Podobno sliko dobimo pri primerjavi razširjenosti po kontinentih; največja je v Evropi in Aziji.

V Sloveniji je stanje varovanja informacij precej odvisno od panoge. Največja ozaveščenost je v finančni dejavnosti in vladnih institucijah, pomena standarda oz. vzorno urejenega sistema varovanja informacij pa se vse bolj zavedajo tudi druge organizacije, predvsem veliki izvozniki.

Za največjo ozaveščenost državne uprave in bančno-finančne dejavnosti so pravzaprav najbolj zaslužni regulatorji teh področij. V finančni industriji sta to Banka Slovenije, ki je že leta 2000 izdala odločbo o nujnosti upoštevanja priporočil prvega dela standarda BS 7799, PSIST BS 7799. Ravno tako velja za akterje borznega trgovanja, t.j. borzno posredniške hiše in družbe za upravljanje, odredba Agencije za trg vrednostnih papirjev (ATVP), da morajo imeti pripravljen in uveden sistem okrevanja po katastrofi. Podobno vlogo kot Banka Slovenije in ATVP je v državni upravi opravil Center vlade za informatiko s priporočili za urejanje informacijske varnosti, ki so povzeta po prvem delu standarda ISO 17799.

V gospodarstvu prihajajo vzpodbude in impulzi ozaveščanja s trga. Tuji partnerji in veliki kupci se že spogledujejo z zahtevami po izkazovanju sposobnosti varovanja informacij. Vsako partnerstvo namreč zahteva izmenjavo informacij, mnogokrat poslovnih skrivnosti. Zahteva po sposobnosti njihovega varovanja je potemtakem povsem legitimna.

V slovenščino je preveden le zgoraj omenjeni standard PSIST BS 7799 iz leta 1995, to je prevod prve izdaje tega standarda. Letos je slovenski inštitut za standardizacijo že izdal oba aktualna dela standarda v angleščini, pripravlja pa tudi oba prevoda, ki bosta najverjetneje izšla v začetku prihodnjega leta.

Sklep

Varovanja informacij se torej lahko različno lotimo. Naslonimo se lahko na svoje znanje in logično razmišljanje, lahko pa uporabimo priporočila različnih standardov, najboljših praks, procedur in postopkov. Ena od možnosti je standard ISO 17799/BS 7799-2, ki prinese uporabniku številne prednosti, med njimi najboljšo prakso upravljanja varnosti informacij, mednarodno priznano izkazovanje sposobnosti varovanja informacij, nenehno izboljšujoč se sistem kot tudi možnost certificiranja oziroma neodvisnega prikaza skladnosti. Standard z vztrajanjem na določenih zahtevah (analiza tveganj) omogoča investirati varnostni tolar na prava, najbolj akutna mesta, optimizira poslovna partnerstva in olajša uvedbo najsodobnejših tehnologij v poslovanje. Z upravljanjem varovanja informacij po standardu ISO 17799/BS 7799-2 in pridobitvijo certifikata zadostimo tudi zakonskim zahtevam.

▪

Rado Ključevšek, soustanovitelj in direktor podjetja K.Sec, d. o. o., je diplomiral na dveh smereh študija računalništva in kasneje magistriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani s področja kriptologije. Doslej je delal kot projektni vodja za razvoj kriptografskih sistemov na MNZ, kasneje je bil svetovalec vlade, zadolžen za varovanje informacij na MF, ter vodja področja informacijske varnosti pri Zaslonu in kasneje Hermes SoftLabu. Njegovo delo obsega svetovanje o informacijski varnosti, upravljanje z varnostjo informacij po standardu ISO 17799/BS7799, razvoj kriptografskih in PKI rešitev ter sodelovanje pri rešitvah za e-poslovanje. Vodil je razvoj orodja Poslovni ŠČIT. Je vodilni presojevalec za standarde BS 7799 ter ISO 9001.

Zaupanja vredno računalništvo
(Trustworthy Computing)

Mnoge tehnologije, ki temeljijo na uporabi računalnikov, veljajo danes za izredno zanesljive in zaupanja vredne. Računalnikom smo zaupali pri poletih na luno, vsak dan jim zaupamo upravljanje kritičnih sistemov za usmerjanje letalskih poletov, finančne transakcije trilijonov dolarjev na dan, shranjevanje dokumentov na osebnih računalnikih itn. Kljub temu računalništvo še ni doseglo točke, ko bi mu ljudje brez pomislekov zaupali svoje življenje, osebne informacije ter pomembne finančne in zdravstvene podatke. Če so se mnoge tehnologije izkazale za izredno zanesljive in zaupanja vredne, kot so na primer elektrika, telefoni in avtomobili, so ljudje še vedno zaskrbljeni zaradi varnosti in zanesljivosti računalniških sistemov. V času, ko je računalništvo povsod navzoče, se še dodatno povečuje pomen prizadevanj, da bi računalniški ekosistem postal tako zaupanja, da ljudje ne bi bili več zaskrbljeni zaradi morebitnih napak ali nezanesljivosti.

Razvoj varnih računalniških sistemov danes dodatno otežuje še hiter razvoj interneta in njegovega povezovanja z zasebnimi omrežji. S tem se brišejo ali zamegljujejo varnostne meje, saj se zaupni in pomembni podatki splošno prenašajo, do njih pa uporabniki dostopajo v zasebnih poslovnih omrežjih in zunaj njih. Pojavile so se tudi nove nevarnosti, ki jih pionirji današnjih sistemov in omrežij niso mogli predvideti.

Kot vodilno podjetje na področju računalništva se Microsoft zaveda svoje odgovornosti pri doseganju razvojne stopnje, ko se bodo ljudje brez pomislekov zanesli na delovanje mikroprocesorjev v vsaki napravi, kot se danes brez pomislekov zanašajo na elektriko.

Dosedanje iniciative v računalništvu so se ponavadi osredotočale na posamezna ozka področja, na primer na zaupanje pri e-poslovanju, toda resnično učinkovit pristop mora vsebovati tako tehnična in družbena vprašanja kot tudi vedenje uporabnikov. Najprej bo treba razviti tako zanesljivo strojno opremo, da jo bo mogoče uporabiti v vseh napravah, ali z drugimi besedami – pri računalniški strojni opremi ne sme prihajati do napak pogosteje kot pri podobno pomembni tehnologiji iz vsakodnevnega življenja. Nato je treba pozornost nameniti programski opremi, ki upravlja s strojno opremo, in navsezadnje tudi storitvam.

»Da bi računalniki postali samoumevni, morajo postati dostopni kjerkoli in kadarkoli jih ljudje potrebujejo, zanesljivo morajo ščititi osebne podatke pred zlorabo ter ponuditi ljudem nadzor nad uporabo njihovih podatkov in biti nezmotljivo varni. Ta koncept imenujemo zaupanja vredno računalništvo (Trustworthy Computing)[1].«

Zaupanja vredno računalništvo je torej dolgoročna vizija razvoja, ki opisuje čas, ko se bodo ljudje lahko zanesli na svoje računalniške sisteme enako, kot se danes zanesejo na elektriko ali telefon. Za Microsoft pa je zaupanja vredno računalništvo tudi vse podjetje obsegajoča iniciativa, ki spreminja način njegovega delovanja na vseh področjih.

V Microsoftu so v okviru iniciative zaupanja vrednega računalništva identificirali štiri cilje, ki jih je treba izpolniti za zaupanja vredno računalništvo: varnost, zasebnost, zanesljivost in poslovna integriteta. Ko bodo doseženi ti cilji, bodo uporabniki lahko pričakovali, da so računalniški sistemi odporni na napade in da so zavarovani zaupnost, integriteta ter razpoložljivost sistema in njegovih podatkov (varnost). Uporabniki bodo lahko nadzorovali podatke o sebi in uporabo leteh (zasebnost) ter upravičeno pričakovali, da bo izdelek opravil svojo funkcijo, ko ga bodo potrebovali (zanesljivost). Cilj poslovne integritete pa zahteva, da so ponudniki izdelkov dostopni in odgovorni.

Da bi uresničil omenjene cilje, Microsoft razvija sisteme, ki so varni v zasnovi, med razvojem in v namestitvi. Rešitve, ki odstranjujejo nekatere šibke točke, kot so na primer gesla ali lažna e-poštna sporočila, že obstajajo, vendar niso dovolj. Microsoft je zato temeljito spremenil način razvoja programske opreme, delovanja in poslovne prakse ter podporo uporabnikom.

Do nedavnega je računalniška industrija največ pozornosti namenjala novim zmogljivostim in funkcionalnostim programske opreme. Četudi Microsoft še vedno veliko vlaga v razvoj novosti, ki jih uporabniki zahtevajo, pa imajo varnostne izboljšave prednost pred vključevanjem novih možnosti. V ta prizadevanja sodijo na primer spremembe v programu Microsoft Outlook, ki zavrne priponke, povezane z nevarnimi datotekami, preprečuje dostop do stikov in daje administratorjem možnost upravljanja z varnostnimi nastavitvami.

[1] *Bill Gates, Computing You Can Count On, april 2002. http://www.microsoft.com/presspass/ofnote/04-21billgessay.asp.*

Microsoft izvaja tudi zahtevne in obsežne preglede mnogih izdelkov, da bi odpravil ostale morebitne varnostne pomanjkljivosti. V začetku leta 2002 so ustavili razvojno delo več kot 8.500 inženirjev in opravili obsežno varnostno analizo milijonov vrstic izvorne kode operacijskega sistema Windows. Vsi inženirji za Windows in več tisoč inženirjev iz drugih oddelkov podjetja se je udeležilo posebnih izobraževanj za pisanje varne programske opreme. Prvotno so pričakovali, da bo ustavitev trajala trideset dni, vendar so z razvojem nadaljevali šele po skoraj dveh mesecih in vložili več kot sto milijonov dolarjev. Podobne preglede kode in varnostna izobraževanja so opravili tudi za Microsoft .NET, Microsoft Visual Studio .NET, Microsoft Office, Microsoft SQL Server, Microsoft Exchange Server, Microsoft BizTalk Server, Microsoft Systems Management Server, Microsoft Host Integration Server, Microsoft Commerce Server in Microsoft Content Management Server.

Pri razvoju se je Microsoft posvetil občutljivosti izdelkov, kot je Windows .NET Server, za napade s spremembo začetnih nastavitev, pri čemer je onemogočil več kot dvajset storitev in komponent, ki se ne uporabljajo pogosto, ter zmanjšal privilegije mnogih drugih.

Spremembe načina razvoja programske opreme so se dotaknile vseh faz razvojnega procesa. Spremenjeni razvojni procesi občutno zmanjšujejo pogostost napak v programski opremi in pospešijo razvoj novih izdelkov ter storitev.

Microsoft ponuja uporabnikom orodja in vire za pomoč pri zagotavljanju varnosti v okoljih Windows. Poslovnim uporabnikom so na voljo orodja za varnostno upravljanje Software Update Services (SUS), ki omogočajo administratorjem hitro in zanesljivo nameščanje kritičnih popravkov izza poslovnega požarnega zidu na strežnike ter namizja. Pogoste napake pri varnostnih nastavitvah lahko uporabniki analizirajo z orodjem Microsoft Baseline Security Analyzer. Orodje omogoča tudi iskanje manjkajočih varnostnih popravkov in pomanjkljivosti v različnih izdelkih, med drugim v novih različicah izdelkov Internet Information Server, SQL Server ter Office.

Prek možnosti za sporočanje napak, ki so vgrajene v paket Office XP in operacijski sistem Windows XP, pridobi Microsoft množico povratnih informacij in jasnejši pregled nad problemi, s katerimi se srečujejo uporabniki. S temi informacijami je mogoče izboljšati tako delovanje Microsoftovih izdelkov kot tudi izdelkov drugih ponudnikov. Na varni spletni strani lahko ponudniki programske in strojne opreme pridobijo podatke o napakah, povezanih z njihovimi gonilniki, orodji in aplikacijami. Možnosti za poročanje nadgrajuje Microsoft Update, ki omogoča več kot tristo milijonov prenosov najnovejših popravkov in izboljšav.

Priznanje za dosedanje delo pri razvoju varnih izdelkov je Microsoft dobil oktobra 2002, ko je organizacija International Standards Organization (ISO) potrdila, da operacijski sistem Windows 2000 izpolnjuje ali presega varnostne zahteve za komercialno dostopne sisteme. Windows 2000 je na podlagi kriterijev ISO Common Criteria for Information Technology Security Evaluation prejel certifikat Evaluation Assurance Level4+ Flaw Remedation. Sistem preizkušanja in certificiranja Common Criteria je mednarodno priznan standard, ki uporabnikom omogoča ocenjevanje varnosti izdelkov IT.

Pri ustvarjanju zaupanja vrednega računalništva stavi Microsoft na večplastni pristop, ki v proces varnosti poleg podjetja vključuje tudi partnerje in stranke. Na tem področju je potrebnega še veliko dela, saj morajo tudi uporabniki sami poskrbeti za svojo varnost, kar vključuje tako odgovorno obnašanje na spletu kot tudi posodabljanje programske opreme, to pa zagotavlja zaščito pred virusi. Microsoft k sodelovanju spodbuja tudi svoje partnerje in jim ponuja številne vire, ki jim omogočajo razvoj varnejših rešitev skrbi za uporabniške potrebe. Zaupanja vredno računalništvo je obveznost za vso industrijo in uporabnike, saj bodo lahko le tako računalniki postali pomemben in zanesljiv del našega vsakdana.

Četudi je bilo opravljenega že veliko dela, bodo mnogi problemi tudi v prihodnosti zahtevali podrobno raziskovalno delo. Zaupanja vredno računalništvo je namreč večplastni skupek prizadevanj, ki jih ne more uresničiti računalniška industrija sama, ampak zahteva sodelovanje vse ekonomije in družbe. Brez obširnega sodelovanja med ponudniki strojne ter programske opreme, akademskimi institucijami in vladami se ne bo mogoče učinkovito spopadati s prihodnjimi izzivi.

Slovensko društvo INFORMATIKA

zbira na podlagi 53. člena statuta in pravilnika o priznanjih
predloge za
priznanja Slovenskega društva INFORMATIKA

1. Priznanje se lahko podeli posamezniku ali pravni osebi za:

- dosežke na področju uporabne in znanstvene informatike ter vidne prispevke na področju razvoja informacijske družbe in razvoja novih načinov in tehnologij dela na področju informatike,
- dolgoletno uspešno delo v društvu ali v drugih društvih, ki so sodelovala z društvom pri programskih vprašanjih,
- razvoj mednarodnega sodelovanja in izmenjavo dosežkov na tem področju,
- izjemne dosežke na področju razvoja konceptov, programskih orodij, naprav in tehnologij v zvezi z informatiko,
- uspešno sodelovanje z društvom,
- publicistično delo na področju informatike in informacijske družbe in
- izjemne dosežke na področjih, ki zadevajo vprašanja informatike.

2. Predlog mora vsebovati:

- podatke o prejemniku priznanja,
- opis dosežka,
- predlagano priznanje,
- dokazila o dosežku,
- podatke o predlagatelju.

Podrobni pogoji so navedeni v pravilniku na naslovu http://www.drustvo-informatika.si

Predloge pošljite do vključno 30. januarja 2004 na naslov:

Slovensko društvo INFORMATIKA
1000 Ljubljana, Vožarski pot 12
z oznako "PRIZNANJA 2004"

Predloge bo v skladu s pravilnikom obravnavala komisija za priznanja in jih s svojim mnenjem posredovala izvršnemu odboru društva. Priznanja bodo javno podeljena na otvoritvi posvetovanja Dnevi slovenske informatike aprila 2004.

Ponovno vas vabimo, da si rezervirate čas za udeležbo na posvetovanju

XI. DNEVI SLOVENSKE INFORMATIKE

14.–16. aprila 2004

Kongresni center Grand hotela Emona, Portorož

predavanja domačih in tujih strokovnjakov

▪

okrogle mize

▪

delavnice

▪

razstave

▪

družabni dogodki

Program posvetovanja:

poslovna informatika in elektronsko poslovanje

▪

informacijske tehnologije in internet

▪

informacijska kultura in družba

Informacije: **www.dsi2004.org**

International Symposium on Performance Analysis Systems and Software (ISPASS-2004)	10.–12. mar. 2004	Austin, Texas, ZDA	IEEE	http://ispass.org
2nd Easterrn Eurrope edGov Day 2004	12. mar. 2004	Budimpešta, Madžarska	Forum e-Government of the Austrian Computer Society (OCG)	http://egov.ocg.at/eeegovday04.html
2nd International Symposium on Code generation and Optimization (CGO 2004)	20.-24. mar. 2004	Palo Alto, San Jose, California, ZDA	ACM - SIGMICRO, IEEE	http://www.cgo.org
ACM International Conference on Computing Frontiers (CF '04)	14.–16. apr. 2004	Ischia, Italija	ACM - SIGMICRO	http://www.computingfrontiers.org beaty@emess.mscd.edu
5th Working Conference on Knowledge Management in Electronic Government (KMGov2004)	17.–19. maj 2004	Krems, Avstrija	Krems Danube University Krems, IFIP WG 8.3 & WG 8.5	http://falcon.ifs.uni-l inz.ac.at/kmgov2004 /http://falcon.ifs.uni-linz.ac.at wimmer@ifs.uni-linz.ac.at
ACM SIGPLAN Conference onLanguages, Compilers, and Tools for Embedded Systems (LCTES'04)	11.–13. jun. 2004	Washington, ZDA		http://www.acm.org/sigplan/lctes. htmhttp://lctes04.flux.utah.edu
31st Annual International Symposium on Computer Architecture - ISCA-2004	19.–23. jun. 2004	München, Nemčija		http://isca.in.tum.de/
16th Euromicro Conference on Real-time Systems (ECRTS 04)	30. jun.–2. jul. 2004	Catania, Italija	Euromicro Technical Committee on Real-time Systems	http://www.diit.unict.it/ecrts2004
IFIP World Computer Congress (WCC 2004)	22.–27. avg. 2004	Toulouse, Francija	IFIP	http://www.wcc2004.org dervillers@wcc2004.org
WCCE 2005-World Conference on Computers in Education	4.–7.jul. 2005	Južna Afrika	IFIP	http://www.wcce2005.org.za

Včlanite se v Slovensko društvo INFORMATIKA

Pristopna izjava

Želim postati član Slovenskega društva INFORMATIKA

Prosim, da mi pošljete položnico za plačilo članarine SIT 6.700 (kot študentu SIT 2.900) in me sproti obveščate o aktivnostih v društvu.

(ime in priimek, s tiskanimi črkami)

(poklic)

(domači naslov in telefon)

(službeni naslov in telefon)

(elektronska pošta)

Datum: Podpis:

Članarina SIT 6.700,- (plačljiva v dveh obrokih) vključuje tudi naročnino za revijo Uporabna informatika. Študenti imajo posebno ugodnost: plačujejo članarino SIT 2.900,- in za to prejemajo tudi revijo. Izpolnjeno naročilnico ali pristopno izjavo pošljite na naslov:
Slovensko društvo INFORMATIKA, Vožarski pot 12, 1000 Ljubljana.

Lahko pa izpolnite obrazec na domači strani društva: **http://www.drustvo-informatika.si**

Naročilnica na revijo UPORABNA INFORMATIKA

Revijo naročam(o)
- ☐ s plačilom letne naročnine SIT 5.900
- ☐ izvodov po pogojih za podjetja SIT 17.800 za eno letno naročnino in SIT 11.900 za vsako nadaljnjo naročnino
- ☐ po pogojih za študente letno SIT 2.800

(ime in priimek, s tiskanimi črkami)

(podjetje) (davčna številka)

(ulica, hišna številka)

(pošta)

Datum: Podpis:

Naročnino bomo poravnali najkasneje v roku 8 dni po prejemu računa.

INTERNET

Vse bralce revije obveščamo, da lahko najdete domačo stran društva na naslovu: **http://www.drustvo-informatika.si**
Obiščite tudi spletne strani mednarodnih organizacij, v katere je včlanjeno naše društvo: IFIP: **www.ifip.or.at,** ECDL: **www.ecdl.com,** CEPIS: **www.cepis.com**

PopoIn
E-Business Suite

Vse aplikacije zasnovane enotno.
Vse informacije na enem mestu.

ORACLE®

www.oracle.si

Razprave

Rešitve

Poročila

ISSN 1318-1882

9 771318 188001