Maja Bolle

Strokovni članek

INFORMACIJSKA VARNOST IN ODPRTOKODNA PROGRAMSKA OPREMA

INFORMATION SECURITY AND OPEN SOURCE SOFTWARE

Professional article

Povzetek Informacijska varnost je ob vedno večji odvisnosti od računalniških sistemov pomembna tema tudi za javno upravo. Ob vedno večjem številu napadov in drugih posegov v integriteto operacijskih sistemov in drugega programja so se mnoge države odločile za prehod na odprtokodno programsko opremo, ki poleg varčevanja pri nakupu programskih licenc državam omogoča tudi večji nadzor nad to opremo. Nekatere raziskave govorijo v prid varnosti zaprtokodnih sistemov, spet druge priporočajo uporabo odprtokodnih. Podatki kažejo, da ima odprtokodna programska oprema na marsikaterem področju boljše varnostne mehanizme kot zaprtokodna, vendar pa ima tudi svoje omejitve. Zaradi teh mora biti prehod držav na odprtokodno programsko opremo dobro premišljen.

Ključne besede ***Odprta koda, odprtokodna programska oprema, zaprtokodna programska oprema, informacijska varnost.***

Abstract In time of increasing dependence on computer systems, information security emerges as an important issue for public administrations. Many governments have made a transition to open source software; the reason being not just financial, but connected to increasing numbers of operating systems security issues. Having more control over the systems is also key. Some research speaks in favor of proprietary software, other in favor of open source software. Data shows that open source software leads over proprietary software in security mechanisms, although they are not without limitations. That is the reason that states transitioning to open source software adoption must take precaution in doing so.

Key words ***Open source, open source software, proprietary software, information security.***

Uvod

Smo v dobi, ko življenje in predvsem delo brez računalnika nista več mogoči. Prav zato je to tudi čas, ko je v ospredju vprašanje informacijske varnosti. Zaradi vedno večjega števila posegov v integriteto najbolj uporabljenih operacijskih sistemov in drugega programja so številne države našle rešitev v prehodu na odprtokodno programsko opremo. Nekatere to pot še iščejo – med njimi je tudi Slovenija. Večina držav se je za prehod na odprtokodno programsko opremo odločila zaradi finančnih razlogov, ne gre pa zanemariti tudi varnostnih (Kimberly, 2005). V članku skušam čim širše predstaviti vprašanje varnosti odprtokodne programske opreme.

Odprtokodna programska oprema (OKPO) je izraz za programsko opremo, katere izvorna koda je prosto dostopna in jo je mogoče prosto uporabljati, raziskovati njeno delovanje, spreminjati in razširjati njene izvirne kot tudi dopolnjene in spremenjene kopije, v primerjavi z zaprtokodno programsko opremo, pri kateri našteto ni mogoče. Pogoji njene uporabe so napisani v različnih licencah, ki vsebujejo smernice uporabe Open Source Initiative. Najpomembnejša merila so prosto razširjanje, dostop do izvorne kode in dovoljenje za spreminjanje ter integracijo te kode (http://www.opensource.org/). OKPO je v uporabi in se razvija predvsem v državah v razvoju (Kshetri, 2004), ponuja jim cenejšo in varnostno zanesljivejšo alternativo zaprtokodnim sistemom.

1 ZGODOVINA IN FILOZOFIJA ODPRTE KODE

Začetki OKPO segajo v petdeseta leta 20. stoletja. Teza, da so ljudje od nekdaj plačevali za programsko opremo, je napačna. Prvi računalniki so bili izjemno veliki, nezmogljivi glede na današnje standarde, predvsem pa so imeli izjemno slabo programsko opremo. Prvi računalnik, ki je bil na voljo za komercialno uporabo, je bil IBM 701 iz leta 1952, za katerega je moral uporabnik na mesec plačevati 15.000 dolarjev uporabnine. Zaradi visoke cene si ga je lahko privoščilo le Ministrstvo za obrambo ZDA, kjer je dobil vzdevek »obrambni kalkulator«. Poznejša različica je bila 705 iz leta 1953, njena cena je bila 1,6 milijona dolarjev. A bolj kot cena je bila vprašljiva programska oprema teh računalnikov. Uporabniški vmesniki so bili uporabniku neprijazni, pa tudi zmogljivost programske opreme je bila manjša, kot jo je omogočala strojna oprema. Ker je bilo programerjev malo, so se uporabniki začeli združevati in si deliti zamisli in programsko opremo, ki bi bolje izkoristila strojne zmogljivosti ter zadovoljila njihove potrebe. Sčasoma so se ustanovila prva združenja, ki so povezovala takšne zanesenjake – najbolj znano je SHARE iz leta 1955. Proti koncu šestdesetih let se je sistem spremenil. Podjetja, ki so prodajala strojno opremo, so kupcu priložila tudi programsko opremo, ki je bila takrat brezplačna (http://www.computerhistory.org/revolution/mainframe-computers/7/172). Po drugi strani pa se je vedno bolj krepil trg, ki je ponujal plačljivo programsko opremo. Ker so se kupci začeli pritoževati, da ne želijo imeti prednaložene programske opreme, češ da naj ne bi zadovoljevala njihovih potreb in da ustvarja monopol, je ameriško sodišče 17. januarja 1969 v sodbi ZDA proti IBM razsodilo, da prednaložena programska oprema zavira konkurenco na trgu (http://history-of-ibm.co.tv/).

1.1 Nastanek prve odprtokodne programske opreme

1.1.1 Unix

Šele leta 1970 je podjetje DEC na tržišču ponudilo prvi računalnik PDP-11, ki je imel dovolj nizko ceno (11.000 USD), da so ga lahko kupili univerze in raziskovalni inštituti (Weber, 2004). Leta 1969 je Ken Thompson izdelal operacijski sistem na računalniku PDP-7 in ga poimenoval UNICS (Uniplexed information and computing services), pozneje so ga preimenovali v Unix. Unix se je začel širiti po univerzah in raziskovalnih inštitutih. Do leta 1972 je bilo namestitev le deset. Veliko prepoznavnost je doživel, ko sta Ken Thompson in Dennis Ritchie leta 1973 na simpoziju ACM predstavila znanstveni članek na temo Unixa. Po objavi članka je število namestitev skokovito naraslo. Podjetje AT&T, pri katerem je bil Thompson zaposlen, je v Unixu zaslutilo poslovno priložnost in zahtevalo njegovo licenciranje. Prva licenca je bila brezplačna in je uporabnikom dovoljevala še precej svoboščin, vendar AT&T zanjo ni omogočal podpore. V vsaki programski opremi neizbežno prihaja do pojava tako imenovanih hroščev (angl. *bug*), napak v programski kodi, ki vodijo v neželene in nepričakovane izide pri njeni uporabi. Vse to je imelo takojšen vpliv na uporabnike Unixa, ki so se začeli povezovati v skupine, skupaj odpravljati hrošče in Unix izboljševati – tega AT&T s svojo licenco ni predvidel. Vseeno pa je bila koda tako zaprta, da so morale te skupine za dostop do izvorne kode AT&T plačati nekaj sto dolarjev. To je storila tudi raziskovalna skupina BTL, ki je izvorno kodo Unixa prepisala v C-programski jezik, s spremembami v kodi pa omogočila, da je Unix od takrat deloval na kakršni koli strojni opremi in katerem koli računalniku. Prav tako je omogočal, da so uporabniki sami izdelovali gonilnike (angl. *driver*) za tiskalnike in podobno opremo, ki so jo potrebovali pri delu. Do leta 1975 je Unix tekel na več kot petdesetih ustanovah po ZDA (Weber, 2004).

1.1.2 BSD

Pomembno vlogo pri razvoju odprte kode ima kalifornijska univerza Berkeley. Tamkajšnji raziskovalci so leta 1973 pod vodstvom profesorja Boba Fabryja ustanovili oddelek za računalniške znanosti, statistiko in matematiko, na katerem so Unix uporabljali, dopolnjevali in spreminjali. Raziskovalca Bill Joy in Chuck Haley sta razvijala in dopolnjevala Unixovo jedro. Leta 1978 je Joy izdelal več dodatkov za Unix, ki jih je skupaj z jedrom spravil v paket, imenovan Berkeley Software Distribution (BSD), vendar to ni bil samostojni operacijski sistem, temveč distribucija Unixa. BSD je postal zelo priljubljen med študenti in raziskovalci, ti so Unix vedno bolj opuščali in raje uporabljali BSD (Weber, 2004).

Leta 1968 je začel delovati predhodnik današnjega interneta, ARPANET. Sprva je povezoval agencijo ameriškega obrambnega ministrstva DARPA (Defense Advanced Research Projects Agency) in druge raziskovalne ustanove. DARPA je želela prek ARPANET-a komunicirati z drugimi ustanovami, vendar sta bila komunikacija in pošiljanje datotek otežena zaradi nezdružljivosti različnih računalnikov in operacijskih sistemov. Ker bi bilo poenotenje strojne opreme drago, se je DARPA obrnila na razvijalce BSD, da bi razvili programsko opremo, ki bi delovala na vseh strojnih

opremah. Fabry je leta 1979 podpisal pogodbo o razvoju BSD, ki bo deloval po željah DARPE. V ta namen je Univerza Berkeley ustanovila nov oddelek, imenovan CSRG (Computer System Research Group), leta 1981 so za DARPO razvili 4.1 BSD. Naslednja različica, 4.2. iz leta 1983, je vključevala nov protokol TCP/IP za medmrežno komunikacijo, ki ga uporabljamo še danes in je temelj današnjega interneta. Različica 4.2 je bila do takrat najhitreje razširjena, naložena je bila na več kot tisoč računalnikov. Prav internet in protokol TCP/IP sta med glavnimi vzroki, da se je začela distribucija BSD množično širiti po medmrežju. AT&T je medtem vedno bolj zaostroval licenco za Unix in ji s tem višal ceno. Leta 1989 je bila cena licence 250.000 USD, česar si univerze niso več mogle privoščiti in so zato prešle na BSD. Da bi lahko ves operacijski sistem ponudili pod licenco BSD in postali neodvisni od AT&T, so ustvarjalci leta 1981 celotno kodo Unixa zamenjali s svojo (Weber, 2004).

1.1.3 Free Software Fundation

Richard Stallman, ki ga danes poznamo kot ustanovitelja Free Software Foundation, je začel v sedemdesetih letih delati na MIT (Massachusetts Institute of Technology). Delal je na oddelku Artificial Intelligence Lab, kjer so raziskovalci razvijali svojo programsko opremo in njeno varnost preizkušali tako, da so drug drugemu vdirali v računalnike. Zelo kmalu je tudi MIT začel omejevati svobodno nameščanje programske opreme. Stallmanu to ni bilo všeč, vrhunec pa je njegovo nezadovoljstvo doseglo leta 1979, ko je njihov oddelek dobil nove laserske tiskalnike podjetja Xerox. Ker so se v tiskalniku nenehno zatikali papirji, je želel sam popraviti programsko opremo tiskalnika in rešiti težavo, vendar mu podjetje Xerox ni želelo dati izvorne kode. Kmalu zatem je na MIT dal odpoved in ustanovil Free Software Foundation. Cilj te neprofitne ustanove je bil narediti popolnoma brezplačen operacijski sistem, katerega izvorna koda bo na voljo vsem in jo bo mogoče tudi svobodno spreminjati. Operacijski sistem je poimenoval GNU (GNU's Not Unix). Leta 1984 je napisal Manifest GNU, v katerem je razložil pomen besede Free Software. Ta ne pomeni nujno brezplačne programske opreme, temveč prosto programsko opremo: prostost se pri tem nanaša na dostopnost do izvorne kode in možnost njenega spreminjanja (beseda *free* v angleškem jeziku ustvarja semantično zmedo, saj ne razlikuje med brezplačen in svoboden, zato je Stallman rešitev poiskal v španskem izrazu *libre*). (Wynants, 2005) Stallman torej ne nasprotuje temu, da ima programska oprema ceno, s katero se plača programerjevo delo, vendar mora biti v svojem bistvu svobodna. V manifestu je napisal štiri temeljna načela, ki veljajo še danes:

1. svoboda uporabljati program v kateri koli namen (svoboščina št. 0);
2. svoboda proučevati program in ga spremeniti po svoji želji. Pogoj za to je dostop do izvorne kode (svoboščina št. 1);
3. svobodno posredovanje kopij (svoboščina št. 2);
4. svoboda izboljšanja programa in objava izboljšav (ter prilagojenih različic) v korist skupnosti (svoboščina št. 3); pogoj za to je dostop do izvorne kode.

Ker se je Stallman zavedal možnosti izkoriščanja teh temeljnih svoboščin, je licenco še dodelal. Ta je nasprotje copyrightu, imenuje pa se General Public License (GPL). Programska oprema, licencirana pod GPL, nikoli ne more postati lastniška, prav

tako tudi ne spremenjena programska oprema, ki izvira iz prostoprogramske, pa tudi nikakršen del kode programske opreme, licencirane pod GPL, ne sme postati del lastniške kode. Sme se izdati le kombinacija lastniške in proste programske opreme, vendar pod pogojem, da se vse licencira pod GPL (Weber, 2004). GPL-licenca je bila sčasoma dopolnjena (zadnja različica je GPL v3) in je služila kot podlaga drugim, bolj specifičnim licencam (http://www.gnu.org/licenses/licenses.html).

1.1.4 Linux

Svetovno najbolj razširjen odprtokodni operacijski sistem na področju superračunalnikov in strežnikov je Linux, ki ima med superračunalniki 91 odstotkov tržnega deleža, za njim sta Unix s tremi odstotki in Windows z enim odstotkom (http://www.top500.org/stats/list/36/osfam). Največji tržni delež ima tudi na področju strežnikov, kar 70,71 odstotka glede na podatke ankete Security Space 2011 (http://www.securityspace.com/s_survey/data/201104/index.html). Vendar pa ima Linux še vedno najmanjši delež na področju namiznih računalnikov (5,1 odstotka), medtem ko imata Windows 85 odstotkov in Mac OS X 8,3 odstotka tržnega deleža (*http://www.w3schools.com/browsers/browsers_os.asp*).

Linux je nastal leta 1991 pod vodstvom takrat 21-letnega Linusa Torvaldsa. 25. avgusta 1991 je v novičarski skupini *comp.os.minix* najavil namero o razvoju jedra novega operacijskega sistema (angl. *kernel*). 17. septembra je na internetu javno objavil prvo različico Linuxovega jedra operacijskega sistema. Ljudi je javno pozval, naj njegov sistem preizkusijo in ga izboljšajo. Linux je iz dneva v dan dobival več podpornikov in razvijalcev, zato je bila že leta 1994 izdana prva različica 1.0.0. Leta 1996 je bila izdana različica 2.0.0, istega leta pa je Torvalds tudi patentiral blagovno znamko Linux (Weber, 2004). Linux danes teče na praktično vsaki računalniški arhitekturi (namizni računalniki, superračunalniki, strežniki, zapestne ure, igralna konzola Playstation 3 ...) (http://www.Linuxfordevices.com/).

Linux je zgolj jedro operacijskega sistema, zato so razvijalci z vsega sveta zanj razvili še grafični vmesnik, namizja, programe, igrice, gonilnike ... in vse to združili v paket, imenovan distribucija. Distribucije temeljijo na posameznem jedru operacijskega sistema (npr. Linux, BSD ...) in se med seboj razlikujejo po tem, kakšno programsko opremo, namizje in skladišča programske opreme vsebujejo. Najbolj razširjena in priljubljena distribucija Linuxa je Ubuntu, ki naj bi jo, glede na podatke, na namiznih računalnikih uporabljalo več kot 12 milijonov ljudi po vsem svetu (Jose, 2011). Po podatkih DistroWatch je na prvem mestu (http://distrowatch.com/) po številu uporabnikov.

2 VARNOST ODPRTOKODNE PROGRAMSKE OPREME

Varnost je relativna, saj jo vsak posameznik dojema drugače. Podobno je z varnostjo odprto- in zaprtokodnih programskih sistemov. Ali je varnejši tisti sistem, ki ima manj hroščev, ali tisti, ki zelo hitro naredi popravke, oziroma tretji, katerega

ranljivost prizadene manj ljudi? Veliko je raziskav, ki govorijo v prid eni ali drugi rešitvi; večina se osredinja zgolj na enega izmed naštetih vidikov (Laurie, 2006). Moja hipoteza je, da je odprtokodna programska oprema varnejša od zaprtokodne. Problematiko skušam predstaviti v čim širšem kontekstu in na različnih področjih, ki so z informacijsko varnostjo tako ali drugače povezana.

2.1 Veliko število distribucij

Po podatkih Distro Watch (http://distrowatch.com/) je na svetu trenutno 320 distribucij, temelječih na operacijskih sistemih, podobnih Linuxu ali Unixu. Resnično število distribucij je v resnici veliko večje, saj lahko doma vsakdo naredi svojo. Prav veliko število distribucij omogoča, da je verjetnost, da bi bila zlonamerna[1] programska oprema pisana za točno določeno distribucijo, veliko manjša, kot je to pri zaprtokodni programski opremi. V dveh najbolj razširjenih zaprtokodnih operacijskih sistemih niti ne poznamo pojma distribucija, saj vsak posameznik kupi operacijski sistem, ki ga ni v več distribucijah, temveč zgolj v različicah (Apple in njegov Mac OS X z različicami Snow Leopard, Lion ... ter Microsoftov Windows z različicami Windows XP, Vista, 7 ...). Vsaka različica teh zaprtokodnih operacijskih sistemov temelji na drugačnem jedru, s čimer se zmanjša prenosljivost zlonamerne programske opreme med njimi. Vendar pa ima zlonamerna programska oprema, ki je pisana za zaprtokodne sisteme, zaradi majhnega števila različic in monokulturnosti Microsoftovih operacijskih sistemov veliko večjo moč razširjanja, saj se različice spremenijo redkeje, kot je to na odprtokodnih operacijskih sistemih, prav tako je zaradi razlik v kodi manjša verjetnost, da bi zlonamerna programska oprema okužila več distribucij (Espiner, 2006). Z vidika informacijske varnosti je veliko število distribucij, ki je značilno za OKPO, torej prednost.

2.2 Zlonamerna programska oprema

Zlonamerna programska oprema je pisana za točno določen operacijski sistem in njegovo različico, saj se izvorna koda med različicami razlikuje. Razširjenost zlonamerne programske opreme, ki je pisana za zaprtokodne in odprtokodne sisteme, je zelo različna. Do danes poznamo več kot dva milijona primerov zlonamerne programske opreme za operacijske sisteme Windows, 1989 primerov za operacijske sisteme Linux in 48 primerov za Apple Mac OS X (Kalkuhl, 2009). Število primerov zlonamerne programske opreme se je v zadnjih dveh letih zelo povečalo, tako na odprto- kot zaprtokodnih operacijskih sistemih. Zadnja poročila inštituta Kaspersky pravijo, da se je število povečalo predvsem zaradi vedno večje priljubljenosti obeh operacijskih sistemov (http://www.securelist.com/en/analysis/204792161/Kaspersky_Security_Bulletin_Malware_Evolution_2010). Največ »zaslug« za novo število primerov zlonamerne programske opreme na področju operacijskih sistemov Linux ima Googlov Android, ki je mobilni odprtokodni operacijski sistem, temelječ na Linuxovem jedru (Racoma, 2011). Zaradi vedno večje priljubljenosti mobilnih

[1] *Kot zlonamerno razumemo (angl. malware) programsko opremo, ki se želi infiltrirati v računalniški sistem ali ga poškodovati, ne da bi pri tem uporabnik privolil v to (Is a Virus or Malware Infection the Cause of Your Slow Computer?, 2011).*

naprav Android je tudi vedno več zlonamerne programske opreme (Sapronov, 2007). Poročilo prav tako ugotavlja, da je od operacijskih sistemov, podobnih Unixu, najbolj na udaru Linux, ki je tudi najbolj razširjen. Vendar statistike kažejo, da je bil Linux napaden predvsem pri strežnikih, manj pa na področju namizja (Sapronov, 2007; Germain, 2008).

Kljub temu da do danes poznamo 1989 primerov zlonamerne programske opreme za OKPO, je njena življenjska doba zelo kratka in v resnici ne naredi toliko škode, kot je lahko naredi na operacijskem sistemu Windows. Razlog tiči v administratorskem dostopu (super user account – bolj znan kot ROOT, do katerega lahko na Linuxu in drugih Unixu podobnih sistemih dostopamo prek ukaza *sudo* – super user do), ki je v Linuxu, BSD in drugih Unixu podobnih operacijskih sistemih iz varnostnih razlogov samodejno deaktiviran, da ne bi nevešči uporabniki upravljali sistema in ga morebiti pokvarili. (https://help.ubuntu.com/community/RootSudo). V praksi to pomeni, da si določimo geslo, s katerim nam je omogočeno spreminjanje vseh nastavitev v operacijskem sistemu, vključno z nameščanjem in odstranjevanjem programov; brez tega gesla pa v sistemu ne moremo spreminjati skorajda ničesar. Drugače je na operacijskih sistemih Windows. Windows prave blokade administratorskega dostopa z geslom ni poznal vse do različic Vista in 7. Blokada pa še vedno ni tako stroga, saj lahko uporabniki v sistemu spremenijo veliko stvari brez administratorskega dostopa (Schneier, 2006). Applov operacijski sistem Mac OS X temelji na Unixovem jedru, pri katerem je administratorski dostop a priori onemogočen in od uporabnika zahteva geslo, podobno kot Linux, kar je dobra lastnost (http://support.apple.com/kb/ht1528). Če pride do okužbe z zlonamerno programsko opremo na Linuxu, škoda ne bo velika, saj ta oprema ne bo imela administratorskega dostopa za ves sistem, njen učinek bo lokaliziran ali pa ga sploh ne bo (http://librenix.com/?inode=21; Koetzle, 2004). Podobno je bilo ugotovljeno v raziskavi Analysis of the Impact of Open Source Software iz leta 2001 (*cardiffschools.net/QinetiQ_OSS_rep.doc*), v kateri so proučevali vpliv virusov na različne operacijske sisteme: Windows je imel takrat več kot 60.000 virusov, Mac OS X in Linux pa po 40. Čeprav večina virusov, pisanih za Windows, ni naredila velike škode, je več sto virusov povzročilo velikansko škodo. Dve tretjini sta naredili veliko škodo Applovemu Mac OS X sistemu, medtem ko niti eden Linuxovih virusov ni povzročil večje škode oziroma se ni bolj razširil po sistemu (Peeling, 2001). Varnost operacijskih sistemov, podobnih Unixu, lahko kljub temu močno ogrozi tako imenovani korenski komplet (angl. rootkit), ki omogoča prikrit dostop do računalniškega sistema in uporabo administratorskih pravic (Chuvakin, 2003).

Kot vidimo, ni tako pomembno, koliko zlonamerne programske opreme obstaja za nek operacijski sistem, pomembneje je, kako široko in na kakšni ravni lahko prizadene sistem. Microsoft je po zgledu odprtokodnih operacijskih sistemov v različicah Vista in 7 onemogočil administratorski dostop in s tem izboljšal varnost sistema.

2.3 Ali veliko oči res več vidi?

Sistem *veliko oči* (angl. many eyes) je sistem pregleda, s katerim ima (teoretično gledano) vsak uporabnik moč pregleda izvorne kode OKPO – s tem je zmanjšana možnost, da bi OKPO vsebovala zlonamerno kodo, kot so stranska vrata, prek katerih lahko nepooblaščena oseba dobi dostop do sistema.

Zagovorniki OKPO pogosto uporabljajo argument, da sistem *veliko oči* omogoča hitro detekcijo hroščev v kodi. V praksi ni tako, večina uporabnikov danes ni veščih programiranja, izvorne kode ne znajo brati ali v njej prepoznati pomanjkljivosti in morebitnih stranskih vrat. OKPO uporabljajo za vsakodnevna opravila, kot so pisanje besedil, urejanje preglednic, pisanje spletne pošte ... Še vedno pa OKPO omogoča vpogled tistim, ki jih to zanima in so tega sposobni. To je pomembna razlika, saj zaprtokodni sistemi tega ne omogočajo (Laurie, 2006).

V zgodovini je bilo več primerov, da več let niso odkrili ranljivosti, čeprav je OKPO pregledalo več ljudi. Eden zanimivejših primerov so stranska vrata Kena Thompsona, ki je bil razvijalec sistema Unix, v katerega je stranska vrata vnesel sam. Šele po 14 letih je Thompson to razkril. S tem malim eksperimentom je želel pokazati, da se na druge ljudi ne smemo preveč zanašati. Po njegovem mnenju je varna samo tista koda, ki jo napišemo sami (O'Dowd, 2004). Tu se nam poraja vprašanje o človeškem dejavniku. Če je kodo pregledalo veliko ljudi, to še ne pomeni, da je bil pregled tudi dovolj natančen ali da so pregledovalci kompetentni za odkritje vseh ranljivosti.

2.4 Čas za popravek

Čas za popravek je čas med tem, ko zaznamo ranljivost v kodi, in časom, ko se naredi popravek. Ta čas je izjemno pomemben in mora biti čim krajši – dlje kot je ranljivost brez popravka, bolj je varnost sistema ogrožena. Raziskava primerjave varnosti pri operacijskih sistemih Windows in različnih Linuxovih distribucijah (Debian, Red Hat, Mandark) v enem letu je pokazala število zaznanih nevarnosti, čas za izdelavo popravka in število popravljenih nevarnosti (Koetzle, 2004). Windows je za izdelavo popravkov v povprečju potreboval najmanj časa, 25 dni, sledile so mu Linuxove distribucije Red Hat in Debian s 57 dnevi in Mandark z 82 dnevi.

Zgolj ta podatek pa za primerjavo varnosti operacijskih sistemov ne zadostuje: pri Windowsih so našteli največ nevarnosti najvišje stopnje (67 odstotkov vseh nevarnosti), sledil je Red Hat s 56 odstotki nevarnosti enake stopnje. Raziskava je merila tudi čas, ki je potreben, da ponudniki vnesejo popravke v distribucijo. Pri OS Windows je bil ta čas enak kot za izdelavo popravkov, saj distribucij sistemov Windows ni. Debian je v povprečju potreboval zgolj 32 dni, kar je veliko manj od časa, ki ga je potreboval za izdelavo popravkov (57 dni), prav tako Red Hat s 47 dnevi. Debian je bil tako hiter, ker je bil edina proučevana distribucija, ki se posodablja, ne da bi bila potrebna ponovna namestitev celotnega sistema (angl. rolling release). Ko distribucijo enkrat namestimo, je ni treba nikoli več nameščati, saj se ves sistem posodablja

samodejno, skupaj z vsemi nameščenimi programi. Zanimivost se je pokazala tudi pri Microsoftu.

Za varnost ni pomemben samo čas izdelave popravkov, predvsem so pomembni uporabniki, ki si morajo te popravke namestiti. Uporabnike Microsofta je ogrožalo devet ranljivosti najvišje stopnje, vendar večina proučevanih kljub temu popravkov več kot 305 dni ni namestila. To pomeni, da so bili v povprečju ogroženi 305 dni, čepav je Microsoft v povprečju izdelal popravke že po 25 dneh (Koetzle, 2004). Podatek lahko kaže na nižjo računalniško pismenost uporabnikov operacijskega sistema Windows v primerjavi z uporabniki Linuxa.

Če ljudje prek sistema *veliko oči* v OKPO odkrijejo ranljivost, to nemudoma objavijo na posebnih spletnih straneh, forumih ipd. (zelo znana taka stran Linuxove distribucije je Ubuntu Bugs Launchpad – https://bugs.launchpad.net/ubuntu/). Razvijalci OKPO ranljivost nato čim hitreje odpravijo. Seveda obstajajo razlike med razvijalci različnih OKPO. Apache v povprečju izdaja popravke vsak dan, tako da ranljivost redko traja dlje od enega dneva. Ubuntu, ki je najbolj razširjena Linuxova distribucija, popravke izdaja glede na prednostni vrstni red, ki se določi prek Ubuntu Bug Launchpad.

Ponudniki distribucij odprtokodnih operacijskih sistemov navadno malce zaostajajo za razvijalci. Tako na primer profesionalni odprtokodni program za 3D-animacijo Blender (http://www.blender.org/) na svoji spletni strani ponuja različico 2.57, medtem ko uporabniki operacijskega sistema Ubuntu prek programskega središča lahko namestijo različico Blender 2.49. Ponudniki svojih baz torej ne osvežujejo skladno z vsakodnevnim razvojem OKPO. To pomanjkljivost odpravlja *skladišče programske opreme* (angl. repository), ki uporabnikom omogoča, da najnovejšo različico programa namestijo neodvisno od ponudnikov distribucije in v trenutku, ko jo razvijalec objavi. Skladišče programske opreme je bilo narejeno za hitrejše posredovanje najnovejše različice programske opreme ter hitrejšo pridobitev povratne informacije o kakovosti te opreme, ki zelo hitro pride do razvijalca, kar pospeši njen razvoj (Laurie, 2006). Leta 2007 je Ubuntu izdal programsko opremo Personal Package Archive (PPA) z namenom, da bi še pospešili in olajšali distribucijo programske opreme prek skladišč (Humbrey, 2011). Ni nujno, da so vsa skladišča varna, saj si lahko dodamo skladišče, ki vsebuje zlonamerno kodo. Zato je priporočeno, da se dodajajo samo skladišča, ki so preverjena in niso sumljivega porekla.

Zaprtokodna operacijska sistema Windows in Mac OS nimata sistema *veliko oči*, temveč za varnost skrbijo razvijalci obeh sistemov. Vseh ranljivosti ne objavljajo javno, zato tudi ne vemo, kako dolgo smo dovzetni zanje in kakšno je njihovo resnično število.

Kot vidimo, večje število javno objavljenih nevarnosti še ne pomeni bolj ranljivega sistema, temveč preglednejšega. OKPO je s tem v prednosti, saj pri zaprtih sistemih zaradi nepreglednosti sistema ne moremo vedeti za vse varnostne ranljivosti.

2.5 Varnost s preglednostjo ali skrivanjem

Velikokrat slišimo, da skrivanje izvorne kode vodi v večjo varnost, vendar to v resnici ne drži. Že eden prvih kriptologov, Auguste Kerckhoffs, je davnega leta 1883 napisal šest načel dobre kriptografije, kar danes imenujemo Kerckhoffsov zakon; ta pravi, da je dober šifrirni sistem varen, tudi če o njem vemo vse, razen šifrirnega ključa. Kerckhoffs prav tako zavrača načelo, da je varnost mogoče zagotoviti s skrivanjem; ne zahteva, da je šifrirni sistem javen, vendar opozarja, da skrivnost ne zagotavlja večje varnosti, temveč jo celo ogroža (Kovačič, 2006). Skriti sistem lahko ogroža varnost tako, da vsebuje napake, ki bi jih, če bi bil javen, odkrili in popravili. Eden največjih strokovnjakov za informacijsko varnost in kriptolog Bruce Schneier pravi: »Ne spominjam se nobenega kriptografskega sistema, razvitega naskrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.« (Schneier, 2002) Podobno se je zgodilo z zelo znanim primerom podatkovne baze Borland InterBase, v kateri so leta 2000 odkrili stranska vrata (angl. backdoor) takrat, ko je podjetje propadlo in objavilo izvorno kodo programske opreme, ki je bila pred tem lastniška oziroma zaprta. Programerji so ugotovili, da so bila leta 1994 podatkovni bazi namerno dodana stranska vrata, ki so vse do leta 2001 posamezniku omogočala popoln dostop do vseh podatkov in tudi vrivanje podatkov in vsebin z uporabniškim imenom *politically* in geslom *correct*. Še bolj zaskrbljujoče je, da so podatkovno bazo uporabljale bostonska borza in velike korporacije, kot so Motorola, Nokia in Boeing. Na srečo so odprtokodni programerji zelo hitro naredili popravek, ki je ta stranska vrata zaprl (Poulsen, 2001).

V duhu odprte kode tudi Microsoft danes državam omogoča dostop do izvorne kode pod pogoji, ki so napisani v pogodbi Government Security Program. V njej najdemo približno 60 držav, med njimi tudi države Nata, Kitajsko in rusko tajno službo FSB (Espiner, 2010). Vendar je Microsoft tisti, ki določi, ali bo državi razkril izvorno kodo ali ne. Med državami, ki jim Microsoft ne omogoča vpogleda, najdemo Venezuelo, Kubo in druge države, ki so prešle na odprto kodo v javni upravi. Microsoft naj bi se za razkritje izvorne kode odločil iz komercialnih razlogov. Nekateri strokovnjaki opozarjajo na slabost takšnega sistema. Richard Clayton z univerze Cambridge opozarja, da države tako lažje najdejo varnostne ranljivosti, ki jih lahko izrabijo za napad na druge države, saj podatka o ranljivosti ne objavijo javno, zanjo vedo le znotraj sistema, ki ima dostop do izvorne kode. Government Security Program ima tudi to omejitev, da državam omogoča vpogled v izvorno kodo, ne omogoča pa njenega spreminjanja (http://www.microsoft.com/resources/sharedsource/gsp.mspx).

3 PREHOD DRŽAVNIH JAVNIH UPRAV NA ODPRTO KODO

V zadnjem času je vedno več držav, ki se odločajo za prehod na OKPO. Nekatere prehajajo le delno (npr. v nekaterih vladnih agencijah) in uporabljajo zgolj odprtokodno programje, kot so Libre Office ali Open Office namesto Microsoft Office (to so ZDA, Francija, Nemčija, Češka, Makedonija, Južna Afrika in Filipini). Je pa tudi

vedno več držav, ki so se odločile za popoln prehod na OKPO (Kitajska, Rusija, Brazilija, Venezuela, Pakistan, Kuba, Turčija, Malezija in Španija), kar pomeni, da uporabljajo distribucije operacijskih sistemov Linux ali BSD, skupaj s pripadajočo programsko opremo. Večina držav, ki so se odločile za popoln prehod, je ustvarila svoje državne distribucije operacijskih sistemov, ki vsebujejo točno določeno programsko opremo (tisto, ki jo v specifični javni upravi potrebujejo). Te države so zaradi zagotavljanja večje varnosti naredile svoja skladišča, ki jih posodabljajo njihove državne ustanove, vsebujejo pa programsko opremo, ki je bila razvita posebej za državne ustanove. S tem zagotovijo večjo varnost operacijskih sistemov, saj programsko opremo, ki je v skladiščih, pregledajo in razvijajo države same. Varnost je poleg zmanjšanja stroškov eden glavnih razlogov za prehod državnih javnih uprav na OKPO (Lewis, 2006). Ko so leta 1999 prišla v javnost prva poročila, da naj bi ameriška agencija NSA (National Security Agency) vnesla stranska vrata v vsako kopijo operacijskega sistema Windows 95 (Campbell, 1999), so se države zamislile nad varnostjo in nadzorom pri operacijskih sistemih podjetja Microsoft. Zmotile so jih tudi monokulturne monopolistične tendence Microsofta, ki obvladuje več kot 80 odstotkov tržnega deleža na področju namiznih računalnikov. Zaradi tako velikega tržnega deleža ima zlonamerna programska oprema tudi veliko večje možnosti za širitev in uničenje sistema. Microsoft je poleg tega začel kodo dopolnjevati tako, da je omejevala delovanje na drugih sistemih in s tem države *priklenil* nase (angl. vendor lock-in). To je spodbudilo razmišljanje o alternativnih programskih rešitvah, ki bi državam omogočile večji nadzor nad računalniškimi sistemi in večjo preglednost, večjo neodvisnost od Microsofta in možnost razvoja ter prilagajanja sistema svojim potrebam (Geer, 2003). Mnoge so rešitev videle v OKPO.

Nekaj primerov: v Venezueli so razvili svoj operacijski sistem, imenovan Canaima, ki temelji na distribuciji Debian Linux. Državni dekret številka 3390 (http://asl.mct.gob.ve/images/Marco_legal/decreto3390.pdf) veleva uporabo Canaime v javni upravi, prav tako mora biti vsaka posebej razvita programska oprema za javno upravo licencirana pod licenco GPL (torej mora biti odprtokodna) (Cleto, 2004). Hugo Chavez se je za prehod na OKPO (poleg varnosti in želje po neodvisnosti od ZDA in Microsofta) odločil tudi zaradi podatka, da gre 75 odstotkov cene licenčne programske opreme v druge države, 20 odstotkov za podporo tujih agencij in le pet odstotkov ostane venezuelskim programerjem (Proffitt, 2002). Podobne razloge kot Venezuela je imela za prehod še Kuba, katere lastna distribucija operacijskega sistema Nova temelji na Linuxovi distribuciji Ubuntu. Kuba se je za prehod na odprto kodo odločila predvsem zaradi varnosti in nezaupanja v Microsoftove produkte, pa tudi zaradi ameriškega embarga, ki je povzročil, da je bilo na Kubi zelo težko priti do legalnih Windowsovih operacijskih sistemov. Razlog je tudi v ideologiji. Dekan šole za prosto programje na kubanski Univerzi za informacijske znanosti Hector Rodriguez je dejal: »Gibanje prostega programja je bliže ideologiji kubanskega prebivalstva, predvsem zaradi neodvisnost in suverenosti.« (Israel, 2009) Tudi Rusija se odločila za prehod na OKPO, vendar njen prehod še poteka in se bo končal leta 2012 ali najpozneje leta 2015. Kot glavni razlog je Putin navedel željo po večji neodvisnosti od drugih držav pri uporabi lastniške programske opreme (Morozov, 2011).

Ena zanimivejših držav z vidika prehoda na OKPO je Kitajska, ki se je začela za OKPO zelo zanimati že leta 1990, leta 2005 pa je izdelala prvo različico državnega operacijskega sistema distribucije Linux, Red Flag Linux, ki se uporablja v javni upravi. Hkrati so razvili distribucijo Asianux, ki je usmerjena na azijske trge, saj podpira pismenke (Blanchard, 2007). Kitajska, katere gospodarstvo neizmerno raste, z njim pa tudi potrebe po čim bolj lokalizirani programski opremi, ki najbolj zadovolji potrebe lokalnih podjetij, z razvojem lastne programske opreme postaja konkurenčna na svetovnih trgih (Saxenian, 2003). Kitajska je imela nekdaj eno najvišjih stopenj piratstva na svetu, z uporabo OKPO pa se je to začelo manjšati. Na Kitajskem želijo s tem zagotoviti tudi večjo informacijsko varnost in neodvisnost (Lock, 2006).

Evropska unija velja za eno največjih zagovornic uporabe OKPO. Največji odprtokodni projekti in rešitve so nastali na tleh Evropske unije. Linux je naredil Finec Linus Torvalds, programski jezik Python je delo nizozemskega avtorja Guida van Rassuma, sistem upravljanja podatkovnih baz MySQL pa Šveda Michaela Wideniusa in še bi lahko naštevali (Gonzalez-Barahona, 2006). Evropska unija zelo podpira razvoj OKPO, zato so ustanovili The Open Source Observatory and Repository for European public administrations (OSOR), katerega namen je razvijati posebne aplikacije in odprtokodno programsko opremo, namenjeno uporabi v javni upravi znotraj EU. S projektom želijo zmanjšati stroške v javni upravi, standardizirati formate in postopke povsod po uniji, zmanjšati stroške e-vlade (angl. e-government) in pomagati širiti dobro prakso. OSOR financira Evropska komisija, podpirajo pa ga vlade na nacionalni, regionalni in lokalni ravni (http://www.osor.eu/about).

Na kratko še poglejmo, kje je Slovenija pri uporabi OKPO v državni javni upravi. Leta 2003 je država sprejela dokument *Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev, temelječih na odprti kodi*. V dokumentu lahko preberemo, da bo država podpirala uporabo odprtokodnih rešitev, jih enakopravno obravnavala skupaj z licenčnimi in podpirala izobraževanje za njihovo uporabo (mid.gov.si/mid/mid.nsf/V/.../$file/Politika_OSS_Koncna.pdf*)*. Dokument se zaenkrat še ni uveljavil v praksi. Do letos je država na podlagi raziskave *Ocena ekonomske upravičenosti MS EA za obdobje 2003–2005* (e-uprava.gov.si/eud/e.../Studija%20upravicenosti%20MS%20EA.pdf*)*, ki je ugotavljala, da je licenčna programska oprema finančno bolj smotrna od OKPO, za javno upravo prek javnih naročil kupovala licenčno programsko opremo MS Office. So pa v javni upravi tudi svetle izjeme, kot je na primer Vrhovno sodišče RS, na katerem so v letih 2006 in 2007 opravili prehod in zamenjali pisarniški paket MS Office z Open Office, Microsoftov spletni brskalnik Internet Explorer z Mozilla Firefox in na 4600 delovnih postaj namestili odprtokodno aplikacijo za spletno pošto Thunderbird. Vrhovno sodišče ugotavlja, da na leto tako prihrani približno 400.000 evrov (http://www.finance.si/305469/Sodi%B9%E8a-z-odprto-kodo-prihranijo-400-tiso%E8-evrov-letno/rss1).

Leto 2011 je na tem področju v Sloveniji prelomno, saj je na začetku leta država objavila študijo, s katero izraža namero, da bi do leta 2015 postopoma prešla na

uporabo OKPO; sprva zgolj z zamenjavo MS Office z Open Office, sčasoma pa bi morda zamenjali vse operacijske sisteme z odprtokodnimi, kot so Linuxove distribucije (mju.gov.si/.../Studija_uvajanja_OKPO_na_DP_v_JU_koncna_razlicica_17.2.2011.pdf). Študija je sprožila velik plaz kritik, predvsem ponudnikov licenčnih programskih rešitev, v Microsoftu pa so izjavili, da bi jim takšna odločitev vlade prinesla vsaj 2,5 milijona evrov izgube na leto (Mihajlovič, 2011).

Slovenija je pri uveljavljanju in uporabi OKPO v primerjavi z drugimi državami EU precej zaostala. Vendar je treba tu izpostaviti tudi morebitno problematiko, če bi prišlo do prehoda slovenske državne javne uprave na OKPO. Problematične so aplikacije, narejene posebej za uporabo v javni upravi – narejene so namreč le za Microsoftovo okolje. Do podobnih težav so prišli tudi v drugih državah, saj so morali aplikacije, ki so bile posebej narejene za Microsoftovo okolje, in programe ponovno narediti ali pa jih spremeniti ter omogočiti podporo tudi na drugih operacijskih sistemih in združljivost z drugačnimi formati, kar je povečalo stroške (Souza, 2006).

Znani so primeri prehodov z OKPO nazaj na zaprtokodno programsko opremo. Zelo znan prehod nazaj na Windows Vista je z Dunaja, kjer so se leta 2005 odločili razviti svojo distribucijo, temelječo na Debian Linux, imenovano Wienux. Med glavnimi težavami je bil program Schlaumäuse, ki je bil narejen leta 2003 in namenjen računalniškemu izobraževanju otrok. Program je bil narejen zgolj za okolje Internet Explorer in ni podpiral odprtokodnega programa Firefox. Podjetje, ki je razvilo program, je predvidelo podporo za Firefox šele leta 2009. Dunaj se je zato leta 2008 odločil preiti nazaj na Windows (Mobility, 2008).

Zadnji tak prehod je naredilo nemško zunanje ministrstvo, ki je leta 2005 prešlo na OKPO. Na namizne računalnike so namestili distribucijo Debian Linux. S prehodom so želeli prihraniti denar, ki bi sicer šel za licenčnine. Leta 2007 so v poročilu zapisali, da so s prehodom resnično znižali stroške. Leta 2011 pa so javno najavili, da prehajajo nazaj na MS Windows in MS Office. Kot razlog so navedli pomanjkljivo podporo strojni opremi, kot so tiskalniki in podobno. Stroški se po njihovem mnenju niso zmanjšali, saj so morali veliko denarja vložiti v razvoj lastnih gonilnikov za tiskalnike. Prav tako so se uporabniki pritoževali nad pomanjkanjem funkcij in slabo interoperabilnostjo. Prehod nazaj na MS Windows jih bo po njihovem mnenju stal manj, ker jim ne bo treba plačevati programerjev za razvoj gonilnikov (http://www.h-online.com/open/news/item/No-more-desktop-Linux-systems-in-the-German-Foreign-Office-1191122.html).

4 INFORMACIJSKA VARNOST IN VLOGA OKPO

Vedno pogosteje dobivamo novice o novih kibernetičnih napadih po svetu. Največ pozornosti so deležni napadi, ki potekajo med ZDA in Kitajsko. Vendar kibernetični boji potekajo tudi med mnogimi drugimi državami, saj jim ta asimetrični način bojevanja omogoča dosegati cilje z malo napora in predvsem brez uporabe sile,

čeprav so posledice takšnih napadov lahko tudi hujše (primer Stuxnet). Po podatkih poročila McAfee danes več kot 120 držav razvija ali ima kibernetična orožja za napade na finančne trge, državne računalnike, vojaške baze ... Tipi napadov so različnih vrst, od DDOS in vdorov v sisteme do kraje podatkov. Zaradi povečanega števila napadov je vedno več držav uvedlo posebne centre (poleg CERT), da bi se ob napadih komunikacija med prizadetimi udeleženci izboljšala oziroma bi se na napade hitreje odzvali. Za reševanje te problematike ni enotnega pristopa – vsaka država ima svojega. Deljena so tudi mnenja o tem, kdo naj ima ob napadu na voljo informacije o njem in koliko naj jih bo. Nekateri menijo, da je boljša izključitev javnosti, medtem ko drugi priporočajo čim večjo preglednost (Baker, 2009).

OKPO ima lahko ob napadu veliko moč na defenzivni ravni. Splet zaradi njegove anarhične narave velikokrat poimenujemo »divji zahod« (Baker, 2009). A podobno kot na divjem zahodu se tudi tu vsak posameznik zavaruje s svojim orožjem. Varnost se ob kibernetičnih napadih ne začne na ravni države, temveč na ravni njenih prebivalcev.

Na področju informacijske varnosti prevladujeta dva pristopa, tako imenovana *top-down* in *bottom-up*. Pristop *top-down* izvira iz koncepta nacionalne varnosti in temelji na stvarnosti, v ospredje postavlja državo in njeno vlogo pri pisanju ter sprejemanju zakonodaje, smernic in strategij na področju informacijske varnosti. Za varnost posameznika na področju informacijsko-komunikacijske tehnologije (IKT) mora poskrbeti država, vendar pa lahko državo posredno ali neposredno ogrožajo tudi posamezniki (Svete, 2005). Slabost takšnega sistema je, da zakonodaja zaostaja za prakso in da države v praksi težko ščitijo posameznike na področju varnosti IKT.

Pristop *bottom-up* izvira iz koncepta človekove varnosti, iz liberalistične in konstruktivistične teorije. V ospredje postavlja posameznika z njegovimi vrednotami in interesi. Posameznik na tem področju ni zgolj žrtev, ki jo mora država ščititi, temveč izjemno pomemben dejavnik znotraj informacijske varnosti, ki lahko s svojim delovanjem nanjo močno vpliva. Nevešč posameznik lahko na področju IKT zelo ogrozi varnost, po drugi strani pa lahko zelo vešč k njej veliko prispeva (Svete, 2005).

OKPO na področju informacijske varnosti predstavlja pristop *bottom-up*, saj vsakemu posamezniku daje možnost nadzora nad lastnim sistemom. Za njegovo varnost je odgovoren posameznik, pomembna pa je tudi vloga odprtokodne skupnosti, ki javno opozarja na nevarnosti.

Diver (2007) vidi idealen sistem v kombinaciji obeh pristopov. Države potrebujejo strateške usmeritve in zakonodajo na področju informacijske varnosti, vendar je dobro tudi, da imajo informacijsko bolj vešče posameznike, ki dobro skrbijo za varnost sistema in s tem preprečujejo morebitno širjenje zlonamerne programske opreme.

Sklep OKPO je z leti postala resna konkurenca zaprtokodnim sistemom in prevladuje tako na področjih superračunalnikov kot strežnikov. Rast so opazile tudi države, ki so se med gospodarsko krizo za prehod na OKPO odločile zaradi zmanjšanja stroškov, medtem ko so se nekatere za prehod odločile predvsem zaradi varnosti, nezaupanja v Microsoftove izdelke in v želji po večji neodvisnosti.

Varnost je relativna. V vsak sistem je mogoče vdreti, zato ne moremo trditi, da je nek sistem boljši, drugi pa slabši. Moja hipoteza je bila, da je odprtokodna oprema varnejša od zaprtokodne. Hipotezo delno potrjujem. OKPO ima dobre varnostne mehanizme, vendar je njihova varnost v praksi odvisna predvsem od njenih uporabnikov. OKPO omogoča večjo preglednost in možnost vpogleda v izvorno kodo, vendar to zanima malo ljudi. Večina ljudi uporablja računalnik za preproste zadeve, kot je pisanje dokumentov. Varnost zaupajo razvijalcem OKPO in sistemu *veliko oči*, oba sistema pa v praksi kažeta, da preveč temeljita na zaupanju. Znanih je veliko primerov, ko ranljivosti v sistemu niso bile odkrite več let. Na drugi strani imamo zaprtokodne sisteme, ki običajnemu uporabniku ne omogočajo vpogleda v izvorno kodo in nimajo sistema *veliko oči*. Podobno kot pri OKPO tu varnost temelji na zaupanju do razvijalcev. Razlika med OKPO in zaprtokodnimi sistemi je zgolj v preglednosti, vendar žal oba temeljita na zaupanju ljudi v njuno varnost. Številne države so se zato odločile za OKPO, ker jim omogoča, da izvorno kodo pregledujejo same, poleg tega pa razvijajo opremo, ki je narejena posebej zanje.

Prednost OKPO pred zaprtokodnimi sistemi vidim predvsem na področju javnega objavljanja ranljivosti in hitrega popravljanja pomanjkljivosti.

OKPO ima dobre varnostne mehanizme in omogoča večjo preglednost, za ogroženost sistema pa je še vedno najbolj odgovoren človek. Večina uporabnikov ni vešča uporabe računalnikov. Takšni uporabniki ogrožajo varnost svojih in tujih sistemov, ker ne uporabljajo antivirusnih programov in svoje računalnike neredno posodabljajo.

Hipotetično bi k večji informacijski varnosti OKPO lahko pripomogel pristop *bottom-up*, vendar le, če bi bili vsi uporabniki vešči uporabe računalnikov, če bi znali brati izvorno kodo in iskati ranljivosti, ki bi jih javno objavljali. Takšna pričakovanja so utopična, zato težko trdimo, da je OKPO z varnostnega vidika boljša – ne glede na varnost sistem še vedno ogroža človek.

Trenutno se zaradi svetovne gospodarske krize mnoge države odločajo za prehod na OKPO, predvsem zaradi zmanjšanja stroškov. Tudi Slovenija je med njimi. Na tej točki je nujno izpostaviti morebitne izzive, ki bi se lahko pojavili ob prenagljenem in premalo premišljenem prehodu. Veliko se lahko naučimo iz primerov Nemčije in Dunaja (prehod nazaj na zaprtokodne sisteme zaradi strojne opreme, ki OKPO ne podpira). Zagotoviti bi bilo treba združljivost OKPO in sedanje (ali v prihodnosti načrtovane) strojne opreme – ena izmed možnosti je na primer popis sedanje strojne opreme in preverjanje, kako jo podpira OKPO. Ob morebitni ugotovitvi, da ni podprta, bi bilo treba proučiti stroške razvoja ustreznih gonilnikov. Morda je

največji izziv v programski opremi, ki je pisana zgolj za okolje Windows. Treba bi bilo proučiti stroške razvoja popravkov, ki bi omogočali podporo OKPO, in tudi čas za njihovo izdelavo. Smiselno bi bilo tudi pregledati sedanje distribucije in najti slovenskemu prostoru najustreznejšo (mogoč pa je tudi razvoj domače).

Če Slovenija morebitnega prehoda na OKPO ne bo zastavila premišljeno, se nam lahko zgodi, da se prehod tudi ne bo obrestoval. V Sloveniji je izjemno malo literature na to temo, prav tako znanstvenih člankov in študij. V prihodnje bi bilo koristno opraviti več neodvisnih analiz stroškov in koristi, ki bi ugotavljale smotrnost prehoda Slovenije na OKPO.

Literatura

1. *Baker, S., 2009. In the Crossfire: Critical Infrastructure in the Age of Cyber War. Santa Clara: McAfee, Inc. http://tinyurl.com/3l6k4bm (3 August 2011).*
2. *Blanchard, J. F., 2007. China, multinational corporations, and globalization: Beijing and Microsoft battle over the opening of China's gates. Seoul: Asian perspective. Institute for Far Eastern Studies. http://tinyurl.com/3vb97m4 (2 April 2011).*
3. *Campbell, D., 1999. NSA Backdoor Into Windows. http://tinyurl.com/3k3e4d (12 April 2011).*
4. *Chuvakin, A., 2003. An Overview of Unix Rootkit. Chantilly: iDEFENSE Inc. http://tinyurl.com/42gbmjd (10 September 2011).*
5. *Cleto, S., 2004. Venezuela Embraces Linux and Open Source Software, but Faces Challenges. http://tinyurl.com/3dqh9ns (3 May 2011).*
6. *Diver, S., 2006. Information Security Policy - A Development Guide for Large and Small Companies. Washington: SANS Institute. http://tinyurl.com/3suc5tc (17 September 2011).*
7. *Espiner, T., 2006. Trend Micro: Open source is more secure. http://tinyurl.com/3c6u6cz (20 May 2011).*
8. *Espiner, T., 2010. Microsoft opens source code to Russian secret service. http://tinyurl.com/2w8moaq (3 August 2011).*
9. *Geer, D., in drugi, 2003. CyberInsecurity: The Cost of Monopoly How the Dominance of Microsoft's Products Poses a Risk to Security. http://tinyurl.com/63bhse8 (18 September 2011).*
10. *Germain, J. M., 2008. Linux: A Tempting Target for Malware?. http://tinyurl.com/65jn5vu (1 May 2011).*
11. *Gonzalez-Barahona, J., Robles, G., 2006. Libre Software in Europe. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 161–188.*
12. *Humbery, B., 2011. The Evolution of the Personal Package Archive system. http://tinyurl.com/3tqw8rq (20 May 2011).*
13. *Jose, M., 2011. The Goal is 200 Million Ubuntu Users in 4 Years - Mark Shuttleworth at UDS. http://tinyurl.com/3cd4p67 (23 May 2011).*
14. *Kalkuhl, M., 2009. Malware beyond Vista and XP. http://tinyurl.com/3qemfbs (20 May 2011).*
15. *Kimberly, S., 2005. The value of open standards and open-source software in government environments. Austin: IBM SYSTEMS JOURNAL. Volume 44 Issue 2, January 2005. http://tinyurl.com/3qsatqt (12 May 2011).*
16. *Koetzle, L., 2004. Is Linux More Secure Than Windows? http://tinyurl.com/3p9uue8 (20 May 2011).*
17. *Kovačič, M., 2006. Kriptografija, anonimizacija in odprta koda kot boji za svobodo na internetu. Javnost- the public. Vol. 13. (2006). Fakulteta za družbene vede, Univerza v Ljubljani, p. 93–110.*

18. *Laurie, B., 2006. Open Sources and Security. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 57–71.*
19. *Lewis, J., 2006. Government Open Source Policies – August 2007. Washington: Center for Strategic and International Studies. http://tinyurl.com/3mhva3y (12 May 2011).*
20. *Lock, B. Y., Liu L., Saxena S., 2006. When China Dances with OSS. V C. DiBona, ed. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 197–210.*
21. *Meintjes, T., 2011. Is a virus or malware infection the cause of your slow computer? http://tinyurl.com/442u5se (26 May 2011).*
22. *Mihajlovič, N., 2011. Microsoft gre nad Pahorja, zdaj hoče pošteno konkurenco. http://tinyurl.com/3lxz4va (24 May 2011).*
23. *Mobility, T., 2008. Vienna failed to migrate to GNU/Linux: why?. http://tinyurl.com/6mktzl (9 September 2011).*
24. *Morozov, E., 2011. A Walled Wide Web for Nervous Autocrats. http://tinyurl.com/2vflb3c (29 May 2011).*
25. *O'Dowd, D., 2004. Linux Security Controversy. http://www.ghs.com/linux/security.html (18 September 2011).*
26. *Peeling, N., Satchell, J., 2001. Analysis of the Impact of Open Source Software. http://tinyurl.com/6lyeod8 (19 May 2011).*
27. *Poulsen, K., 2001. Borland Interbase backdoor exposed. Open source reveals foolishly hardcoded password. (12 May 2011).*
28. *Proffitt, B., 2002. Venezuela's Government Shifts to Open Source Software. http://tinyurl.com/3j9kqzo (15 May 2011).*
29. *Sapronov, K., 2007. Kaspersky Security Bulletin 2006: Malware for Unix-type systems. http://tinyurl.com/3vuu2k3 (23 May 2011).*
30. *Saxenian, A., 2003. Government and Guanxi: The Chinese Software Industry in Transiton. Berkeley: University of California at Berkeley. http://tinyurl.com/3u37nwl (12 May 2011).*
31. *Schneier, B., 2002. Secrecy, Security, and Obscurity. Crypto-Gram. http://tinyurl.com/5rk6jaw (17 May 2011).*
32. *Schneier, B., 2006. Microsoft Vista's Endless Security Warnings. http://tinyurl.com/ges4k (23 May 2011).*
33. *Souza, B., 2006. How Much Freedom Do You Want. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 211–229.*
34. *Svete, U. 2005. Varnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.*
35. *Weber, S., 2004. The success of open source. Cambridge: Harward University Press.*
36. *Wynants, M., 2005. Free as in Freedom, not Gratis!. V Wynants, M., Cornelis J., ed. How Open is the Future? Economic, Social & Cultural Scenarios inspired by Free & Open-Source Software. Brussels: Brussels University Press, p. 69–85.*

Viri:

1. *http://distrowatch.com/ (26 May 2011).*
2. *http://librenix.com/?inode=21 (23 April 2011).*
3. *http://support.apple.com/kb/ht1528 (26 May 2011).*
4. *http://tinyurl.com/27l5wvh (26 May 2011).*
5. *http://tinyurl.com/28lpgq (28 May 2011).*
6. *http://tinyurl.com/3f69g8u (19 May 2011).*
7. *http://tinyurl.com/3fldnhr (26 May 2011)*
8. *http://tinyurl.com/3hdqvgd (20 May 2011).*
9. *http://tinyurl.com/3pdksvv (20 May 2011).*
10. *http://tinyurl.com/44x9pxd (26 May 2011).*
11. *http://tinyurl.com/5s4k3ry (10 September 2011).*

12. *http://tinyurl.com/68u2cm7 (12 April 2011).*
13. *http://tinyurl.com/6gyjnou (20 May 2011).*
14. *http://tinyurl.com/6hszcy5 (20 May 2011).*
15. *http://tinyurl.com/6jgg3ut (20 April 2011).*
16. *http://tinyurl.com/hdpo9 (18 September 2011).*
17. *http://tinyurl.com/o4foa (3 May 2011).*
18. *http://www.Linuxfordevices.com/ (20 April 2011).*
19. *http://www.osor.eu/about (20 May 2011).*
20. *https://bugs.launchpad.net/ubuntu/ (18 September 2011).*