REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
POLICIJA

Varni na internetu

Katere nevarnosti nam grozijo, kadar je naš računalnik povezan v internet?

O nevarnostih pri uporabi interneta se je začelo razmišljati s pojavom novih tehnologij, ki so omogočile velike spremembe – ne le pri komuniciranju, temveč tudi pri opravljanju vsakodnevnih nalog. Zaradi teh pridobitev pa smo postali tudi bolj ranljivi. Magnet za napadalce (hekerje, pirate, prevarante, pošiljatelje nezaželenih elektronskih sporočil in podobne »hudobneže«) so postali naši osebni in poslovni podatki ter različna varnostna gesla, z zlorabo katerih lahko naredijo velikansko škodo. Med vsemi grožnjami varnosti na internetu predstavljajo tovrstni napadalci eno največjih. Njihove tarče niso samo vladne ustanove in finančne institucije, temveč tudi podjetja in fizične osebe.

Ko postanemo žrtev elektronskih tatov, posledice običajno niso zabavne. Včasih je potrebno formatirati celoten disk in znova postaviti sistem, včasih pa zaradi naivnosti pri vpisovanju številke svoje kreditne kartice izgubimo zajeten kupček denarja. Še nevarnejši so napadi, ki jih uporabnik ne zazna. Včasih namreč ni nobenega neposrednega znaka, da se nekdo sprehaja po vašem računalniku.

Virusi in nezaželena sporočila

Danes so največja nadloga računalniški virusi (virusi, trojanci in črvi), saj njihovi avtorji z njimi iščejo načine nepoštenega zaslužka, in ne zgolj dokazujejo sebi ali drugim, da jih znajo napisati. Tako dandanašnji virusi zbirajo podatke o geslih in kreditnih karticah, nameščajo trojanske konje ter pošiljajo nenaročena sporočila.

Večino nezaželene pošte (Spam) širijo trojanci, ki preko okuženih osebnih računalnikov v svetovnem spletu pošiljajo nezaželeno pošto. Govor preko internetnega protokola (VoIP) je prinesel nezaželena sporočila tudi na področje neposrednega sporočanja (Spim) in internetne telefonije (Split).

Prav gotovo ste že prejeli obvestilo, da ste nekomu poslali okuženo elektronsko pošto, v vašem elektronskem nabiralniku pa je verjetno že pristalo precej sporočil neznanih pošiljateljev. To pomeni, da ste postali žrtev kraje identitete, imenovane tudi ponarejanje elektronskega naslova oziroma E-mail spoofing. Ta se pojavlja v različnih oblikah, vendar imajo vse enak rezultat. Prejemnik dobi elektronsko sporočilo z enega elektronskega naslova, čeprav sporočilo dejansko izvira s povsem drugega. Večinoma gre za poskus, da bi prejemnike prepričali v izdajo različnih zasebnih informacij.

Parazitni vohunski programi

Delimo jih na Spyware, ki spremljajo naše navade pri brskanju po spletu, in Adware, ki prikazujejo spletne strani z oglasi. Mednje sodijo tudi omrežja za izmenjavo datotek, ki dajejo kapacitete našega računalnika na voljo drugim uporabnikom. V teh omrežjih se datoteke izmenjujejo po principu P2P in so razpršene po številnih računalnikih, ki si iskalno zahtevo podajajo med seboj, dokler datoteka ni najdena.

Vohunski programi se običajno namestijo skupaj z navidez koristnim programom, ki pa je zgolj vaba za naivne uporabnike. So izredno razširjeni in obvladajo zelo dobre tehnike skrivanja, zato jih protivirusna programska oprema ne odkrije. Na računalniku ne kažejo nobenih vidnih znakov, niti ne povzročajo neposredne škode, tako da lahko zelo dolgo ostanejo neopaženi.

Nikoli ne moremo biti prepričani, da je naš računalnik po okužbi z vohunskim programom sploh še varen, saj ne moremo vedeti, kaj ta program dejansko počne v ozadju. Vohunski programi omogočajo napadalcem, da zberejo podatke o žrtvi (npr. sistemske informacije, uporabniško ime in geslo, podatke o spletnih navadah, osebne podatke), ali pa aktivirajo samodejno pojavljanje oglasov in klicne programe (Dialer), ki samodejno kličejo na plačljive telefonske številke ter občutno upočasnijo delovanje računalnika.

Vedno bolj so znane tehnologije Rootkit, ki omogočajo skrivanje datotek, procesov ali drugih objektov, tako da jih uporabniki in tudi aplikacije ne vidijo oziroma ne zaznajo. Napadalci lahko z njihovo pomočjo skrivajo »stranska vrata«, preko katerih izvajajo popoln nadzor nad delovanjem tujega računalnika.

Varnostne napake in brezžična omrežja

Obstaja več različnih tipov varnostnih napak, zaradi katerih lahko napadalci vstopijo v vaš računalnik. Pri tem izkoristijo različne pomanjkljivosti programske in strojne opreme. Orodje, ki bi nas varovalo pred vsemi grožnjami, ne obstaja. Tako imenovani trik Buffer overflow ali preobremenitev medpomnilnika izkoristi napako aplikacije, ki jo je naredil programer.

Poznamo napade na brezžična omrežja WLAN, ki za napadalca niso tvegana, saj napad izvaja z oddaljene lokacije. Ko napadalec s prisluškovanjem zbere dovolj informacij, izvede nedovoljen vstop v brezžično omrežje s tehniko Spoofing. To pomeni, da napadalec zasede vlogo legalne naprave, s tem da se napadenemu sistemu predstavi kot zaupanja vreden sistem.

Napadi za zavrnitev storitve

Poznamo različne modele napadov za zavrnitev storitve, ki jih označujemo s kraticami DoS, DDos in DRDos. Napadalci s pomočjo posebnih skript, imenovanih Boti, pošljejo preko računalnikov, ki jih imajo pod nadzorom (Zombiji), na napaden strežnik veliko količino podatkov. Takšne oblike napadov predstavljajo veliko nevarnost za ponudnike internetnih storitev, saj lahko začasno onesposobijo strežnik ali del omrežja.

Vse pogosteje prihaja tudi do napadov na usmerjevalnike (Router), ki povezujejo lokalna omrežja. Tako lahko napad na en usmerjevalnik onemogoči delovanje celotnega omrežja.

Internetne prevare in zlorabe

Prevaranti najpogosteje privabljajo žrtve preko spletnih strani. Zato je pri kupovanju na spletnih dražbah in plačevanju preko interneta dobro preveriti, kdo zagotavlja varnost pri plačevanju na določeni spletni strani. Med prevarami preko elektronske pošte so najbolj znana nigerijska pisma, kjer nas želijo napadalci prepričati v sodelovanje.

Vedno pogostejši so napadi Phishing, kjer napadalci preko ponarejenih elektronskih sporočil zavajajo osebe oziroma podjetja, da posredujejo zaupne informacije (številke kreditnih kartic, številke računov, PIN kode ipd.) neznani osebi.

Pojavlja se tudi nova tehnika internetnih zlorab Pharming, ki vključuje spreminjanje naslovov sistema DNS, tako da uporabnik ne obišče originalnih spletnih strani, ampak druge, narejene posebej za zbiranje zaupnih podatkov oziroma za krajo identitete.

Spletni klepet

Po svetu obstaja na tisoče kanalov IRC, ki so namenjeni neposrednemu klepetanju med uporabniki interneta. Funkcionalnost sistema omogoča, da strežnik zaradi zasičenosti sistema izloči uporabnika iz sistema. To pa je osnova za napade na IRC-kanale, kjer se hekerske skupine bojujejo med seboj za prevzem kanala ali celo napadejo IRC-operaterja. Napadalce je zelo težko izslediti, saj se lahko omrežja nahajajo v tujini ali na omrežjih brez vzdrževanja.

Hekerji

Po svetu je ogromno računalnikov, ki so pod nadzorom hekerjev. Vsi hekerji so usmerjeni k iskanju informacij, pri tem pa jim informacijska tehnologija predstavlja izziv, ki ga morajo premagati. Razlika med slabimi in dobrimi hekerji je v tem, da eni izkoristijo pridobljeno informacijo za zlonamerno dejanje, drugi pa ne.

Danes je na spletu moč enostavno dobiti programe za odkrivanje gesel, programe za pisanje virusov in skript, s katerimi je mogoče vdreti v računalniški sistem. Tako lahko manjša skupina ali posameznik povzroči več škode kot pred leti jedrsko orožje.

Pornografska vsebina

Pri uporabi interneta so otroci in mladostniki najbolj ogrožena skupina. Zavestno ali povsem po naključju se lahko srečajo s pornografskimi, pedofilskimi in drugimi nezaželenimi vsebinami.

Internet je pravi raj za pedofile, saj jim poleg anonimnosti in skrivanja prave identitete omogoča tudi objavljanje, zbiranje in izmenjavo otroške pornografije prek elektronske pošte, novičarskih skupin, klepetalnic in omrežij za izmenjavo datotek.

Preko interneta lahko pedofili z otrokom vzpostavijo neposredni stik in sčasoma zgradijo trden odnos, temelječ na zaupanju in prijateljstvu, kar lahko kasneje izkoristijo za vzpostavitev fizičnega stika in za zlorabo otrok. Pri svojem početju izkoriščajo otrokove lastnosti, kot so radovednost, zaupljivost in naivnost.

Varovanje avtorskih pravic

Omrežja za izmenjavo datotek so povzročila eno največjih internetnih revolucij zadnjih let, hkrati pa so spremenila tudi glasbeno in filmsko industrijo, saj so omogočila dostop do večine digitalnih vsebin. Poznamo veliko omrežij za izmenjavo datotek (BitTorrent, Direct Connection, IRC, P2P ...), v vsako izmed njih pa se je mogoče povezati z več različnimi programi (uTorrent, DC++, eMule, Kazaa Lite K++, LimeWire, Edonkey ...).

Avtorska dela (računalniški programi, igre, glasba, filmi itd.) so zahtevna za izdelavo, hkrati pa tudi ranljiva glede kopiranja, prenosa in kraje, saj jih je mogoče brezplačno naložiti z interneta. Velika količina piratske vsebine se nahaja na domačih strežnikih, službenih računalnikih in na računalnikih izobraževalnih ustanov. Najbolj neposreden dostop do aktualnega avtorskega dela na internetu predstavljajo strežniki 0-day FTP, klepetalni prostor IRC in omrežja za izmenjavo datotek.

Vsi uporabniki nelegalnih kopij računalniških programov, večpredstavnih vsebin ter uporabniki omrežij za izmenjavo datotek, ki dajejo zaščitena avtorska dela na voljo javnosti in jih razširjajo preko interneta, se s svojimi dejanji izpostavljajo kazenskemu pregonu. Poleg tega uporabniki nelegalnih kopij računalniških programov nimajo dostopa do posodobitev, izboljšav in inovacij, s katerimi lahko zaščitijo svoj osebni računalnik in z njim naredijo več.

Kako se zavarovati?

Izobraževanje in obveščenost

Varnost na internetu je proces, za katerega moramo stalno skrbeti in ga ni moč kupiti. Potrebno je stalno **izobraževanje** uporabnika računalnika o varnosti. Največja napaka večine uporabnikov je nezavedanje o računalniški varnosti in nepremišljeno delo z računalnikom.

Zelo pomembna je **obveščenost** o tem, kaj se dogaja na internetu. Naloga staršev je, da se pogovorijo s svojimi otroki ter jih opozorijo na potencialne nevarnosti, ki jim grozijo na internetu. Opozoriti jih je potrebno, da ni priporočeno vzpostaviti neposrednih stikov preko interneta in posredovati svojih osebnih ter družinskih podatkov neznanim osebam.

Pravilna uporaba in nastavitev programske ter strojne opreme

Na vsakem računalniku je nujna uporaba programov za protivirusno zaščito, filtriranje sumljive pošte in za odstranjevanje vohunskih programov. Nujna je tudi dobra nastavitev in uporaba osebne požarne pregrade (Firewall).

Zagotoviti moramo redno posodabljanje operacijskega sistema, varnostnih programov, spletnega brskalnika in ostale programske opreme s servisnimi oziroma varnostnimi posodobitvami proizvajalca. Priporočljivo je imeti vključeno samodejno posodabljanje sistema.

Vsi spletni brskalniki na obiskani strani puščajo številne podatke. Zato je priporočljivo pogosto brisanje piškotkov (Cookies) in zgodovine obiskanih strani.

Pomembno je, da si delamo varnostne kopije podatkov na zgoščenko, da ne ostanemo brez njih v primeru okužbe z virusom ali poškodovanja strojne opreme.

Na trgu je na voljo ogromno koristnih programov in iger, ki so javni (Public domain) oziroma brezplačni (Freeware). Kljub temu vam svetujemo, da ste pozorni pri prenašanju brezplačnih programov z nepreverjenih spletnih strani.

Uporaba kompleksnih gesel v praksi ne pomaga, če si ne zagotovimo tudi fizičnega varovanja osebnih računalnikov, predvsem prenosnikov.

Za uporabnike brezžičnih omrežij WLAN je priporočljivo, da redno pregledujejo oziroma skenirajo radijsko območje, s čimer lahko pravočasno odkrijejo nepooblaščene dostopovne točke (Access point). Pametno je izklopiti razpošiljanje omrežnega imena SSID, uporabljati močne šifrirne ključe ter spremeniti vsa tovarniško nastavljiva gesla.

Previdnost pri uporabi spletnih strani in elektronske pošte

Večina uporabnikov pri nakupovanju preko spleta ni pozorna na avtentičnost obiskane spletne strani. Zavedati se moramo, da lahko napadalci postavijo svoje spletne strani, ki so vizualno zelo podobne legitimnim spletnim stranem podjetij.

Pri uporabi interneta je nujno, da si zagotovimo svojo anonimnost oziroma da stalno zakrivamo svojo pravo identiteto. V kolikor dostopamo na internet preko javnih dostopnih točk (hotel, kavarna, knjižnica ipd.), moramo paziti, da ne potrdimo možnosti, da bi računalnik shranil naše geslo.

Nikoli ne smemo zaupati identiteti pošiljatelja elektronske pošte, saj se jo da enostavno ponarediti. Zato moramo biti pozorni na elektronsko pošto ne samo neznanega pošiljatelja, čigar identitete ne poznamo, temveč tudi na pošto znanih pošiljateljev, katerih vsebine in priponke ne pričakujemo oziroma smo prejeli pošto z nevsakdanjimi vsebinami. Na takšno pošto ne odgovarjamo, je ne pošiljamo naprej, ne poskušamo odjaviti prejemanja, ne odpiramo priponk oziroma povezave ter jo moramo takoj izbrisati.

Po elektronski pošti nikoli ne posredujemo zaupnih osebnih in finančnih podatkov (davčna številka, številka kreditne kartice, uporabniško ime in geslo ipd.), razen če ni sporočilo digitalno podpisano.

Kdaj storimo kaznivo dejanje?

Neupravičen vstop v informacijski sistem
225. člen KZ RS
Zagrožena je denarna kazen ali kazen zapora do 5 let.

Nezaželena sporočila

Če pošiljate večje število elektronskih sporočil, ki lahko povzročijo oviranje oz. motnje v delovanju informacijskega sistema, lahko s tem storite kaznivo dejanje.

Nezaželena sporočila v Sloveniji urejata Zakon o elektronskih komunikacijah (ZEKom) v 109. členu in Zakon o varstvu potrošnikov (ZVPot) v členu 45.a. Zakon o elektronskih komunikacijah določa, da se nezaželene oglasne pošte ne dovoljuje razpošiljati brez vnaprejšnje privolitve prejemnika, razen če v sporočilu oglašujemo sorodne izdelke ali storitve že obstoječi stranki. Vsako sporočilo mora biti opremljeno z informacijo o brezplačni in enostavni odjavi s poštnega seznama.

Napadi, vdori in nepooblaščeno spreminjanje podatkov

Kdor neupravičeno vdre v informacijski sistem oziroma prestreza ali kako drugače moti oziroma ovira komunikacijo uporabnika, ki se prijavi preko uporabniškega imena in gesla na poštni strežnik, izpolni vse znake kaznivega dejanja Neupravčenega vstopa v informacijski sistem po 225. členu Kazenskega zakonika (gre za 225. člen). Kaznivo dejanje je lahko storjeno samo z direktnim naklepom, kar pomeni, da se mora napadalec zavedati, kaj počne, in imeti namen, da povzroči določeno posledico.

Kazenski zakonik Republike Slovenije vsebuje nekaj členov, ki se posredno ali neposredno nanašajo na vdore v informacijski sistem ali na nepooblaščeno spreminjanje podatkov: Zloraba osebnih podatkov (154/2. člen), Neupravičen vstop v informacijski sistem (225. člen), Vdor v informacijski sistem (242. člen) ter Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (309/3. člen).

Svetujemo vam, da ne uporabljate in ne nameščate orodij oziroma programov, namenjenih za vdor v tuj informacijski sistem. Izogibajte se programov za odstranjevanje zaščite (crack) ter ne izdelujte in ne razpošiljajte računalniških virusov.

Vdor v informacijski sistem
242. člen KZ RS
Zagrožena je kazen zapora do 5 let.

Prikazovanje, izdelava, posest in posredovanje pornografskega gradiva
187. člen KZ RS
Zagrožena je denarna kazen ali kazen zapora do 8 let.

Pornografska vsebina

Kazenski zakonik Republike Slovenije v členu Prikazovanje, izdelava, posest in posredovanje pornografskega gradiva (187. člen) prepoveduje izdelavo, prodajo, prikazovanje ali omogočanje dostopa do predmetov pornografske vsebine in prikazovanje pornografske predstave vsakomur, ki je mlajši od 14 let. Prepovedana je zloraba mladoletne osebe za izdelavo pornografskih predmetov in uporaba mladoletne osebe za pornografsko predstavo. Preko interneta je prepovedano razširjanje in ponujanje otroške pornografije ter posest takšnega gradiva z namenom razširjanja, prodaje in ponujanja.

Avtorske pravice

Če uporabljate računalniški program brez dovoljenja avtorja in se vam dokaže nezakonito reproduciranje ter distribuiranje, ste lahko obsojeni na visoko denarno ali zaporno kazen, poleg tega se vam ob hišni preiskavi zaseže računalniška oprema za reproduciranje. Kaznivo dejanje po prvem odstavku 159. člena Kazenskega zakonika storimo že, če npr. računalniške programe in igre za majhen denar kupimo pri računalniškem piratu in si jih naložimo na trdi disk svojega računalnika, pri tem pa njihova skupna tržna oziroma uradna cena pomeni večjo premoženjsko korist.

Brez dovoljenja avtorja pomeni, da je moral avtor dati izrecno dovoljenje za posamezna dejanja, kar je običajno navedeno v licenčni pogodbi. Kdaj je potrebno dovoljenje avtorja ali drugega imetnika avtorske pravice, določa Zakon o avtorski in sorodnih pravicah (ZASP). Materialne avtorske pravice pa varuje Kazenski zakonik (KZ) v členu Neupravičena uporaba avtorskega dela (159. člen). Dovoljena je uporaba, reproduciranje in distribuiranje brezplačnih programov (Freeware) in brezplačna distribucija preizkusnih programov (Shareware).

Tržna inšpekcija lahko v skladu z Zakonom o avtorski in sorodnih pravicah brez naloga sodišča preišče podjetja, ki so osumljena kršitev avtorskih pravic.

Neupravičena uporaba avtorskega dela in kršitev avtorski sorodnih pravic
159. in 160. člen KZ RS
Zagrožena kazen je denarna kazen ali kazen zapora do 8 let.
Za pravne osebe je denarna kazen do 150 milijonov SIT.

Odkrivanje takih kaznivih dejanj je zaradi svojih značilnosti precej težavno. Kazniva dejanja niso vedno vidna in ne puščajo sledov kot klasična kazniva dejanja, zato jih je težje odkriti. Pri takšnih kaznivih dejanjih pogosto ni mogoče natančno ugotoviti časa izvršitve dejanja, saj je lahko izvršeno v nekaj tisočinkah sekunde. Poleg tega je dejanje lahko storjeno na daljavo. Zato je pomembno, da žrtev kaznivega dejanja zavaruje vse sledi (dnevniške zapise, sporne datoteke itd.), ki bi lahko v nadaljevanju koristile pri identifikaciji storilca kaznivega dejanja in dokazovanju kaznivega dejanja.

Kam se pritožimo?

SI-CERT, TIRS, APEK in BSA

Mnogo uporabnikov interneta išče pomoč ob morebitnih motnjah (ob zaznavi vdora ali poskusa vdora) pri skupini za hitro računalniško pomoč s tega področja, imenovani CERT (Computer Emergency Response Team), oziroma njeni domači enoti SI-CERT (www.arnes.si/si-cert).

Za nadziranje uresničevanja Zakona o varstvu potrošnikov (ZVPot) skrbi Tržni inšpektorat (TIRS), ki deluje v sklopu Ministrstva za gospodarstvo. Prijave kršitve člena 45.a. Zakona o varstvu potrošnikov lahko pošljete na elektronski naslov inšpektorata tirs.info@gov.si, kršitve 109. člena Zakona o elektronskih komunikacijah (ZEKom) pa naslovite na Agencijo za pošto in elektronske komunikacije (APEK).

Poleg omenjenih inštitucij v Sloveniji deluje še organizacija **BSA** (Business Software Alliance), ki nastopa v imenu svetovne industrije komercialne programske opreme pred državnimi organi. Nelegalno uporabo ali prodajo programske opreme lahko prijavite na elektronski naslov **info@bsa.si**.

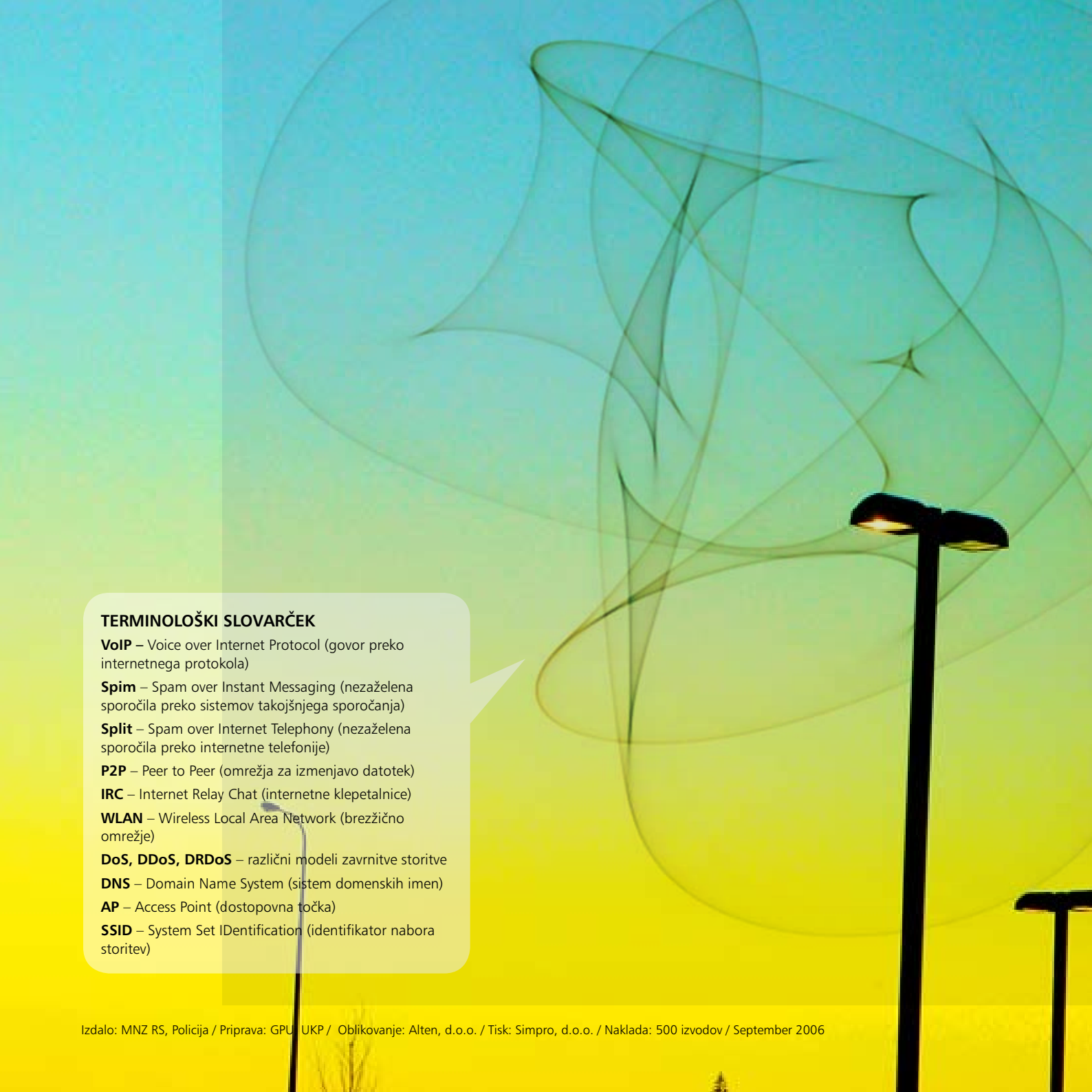
Ponudniki internetnih storitev

Ker večina nezaželene oglasne pošte prihaja izven Slovenije, lahko tržni inšpektorat proti temu stori zelo malo. Pritožbe glede nezaželene pošte lahko naslovite tudi na ponudnika internetnih storitev, kjer je pošta svojo pot začela. Pri tem moramo biti pozorni, saj večina nezaželenih sporočil ne izvira z elektronskega naslova, ki ga vidimo, temveč je pošiljatelj svoj elektronski naslov ponaredil. Za prijavo lahko uporabite posredniško storitev SpamCop (www.spamcop.net), kjer vam bodo analizirali nezaželeno sporočilo in povedali, od kod je bilo sporočilo dejansko poslano. Obvestili vas bodo, na katere elektronske poštne naslove morate poslati pritožbo.

Policija

Policija običajno pridobi podatke o sumu storitve kaznivega dejanja od oškodovancev, ko jim ti naznanijo kaznivo dejanje, bodisi pisno, osebno ali po telefonu. Prijavo lahko podate na Policijski postaji ali v sektorju kriminalistične policije na Policijski upravi.

Pokličete lahko tudi na telefonski številki 113 ali 080 1200 (anonimna prijava). Prijavo kaznivega dejanja lahko podate tudi v elektronski obliki na spletni strani policije (www.policija.si) v rubriki "Pišite nam" oziroma na državnem portalu Republike Slovenije (http://e-uprava.gov.si/e-uprava/dogodkiPrebivalci.euprava?zdid=161&sid=510) v rubriki "E-naznanilo kaznivega dejanja policiji".



TERMINOLOŠKI SLOVARČEK

VoIP – Voice over Internet Protocol (govor preko internetnega protokola)

Spim – Spam over Instant Messaging (nezaželena sporočila preko sistemov takojšnjega sporočanja)

Split – Spam over Internet Telephony (nezaželena sporočila preko internetne telefonije)

P2P – Peer to Peer (omrežja za izmenjavo datotek)

IRC – Internet Relay Chat (internetne klepetalnice)

WLAN – Wireless Local Area Network (brezžično omrežje)

DoS, DDoS, DRDoS – različni modeli zavrnitve storitve

DNS – Domain Name System (sistem domenskih imen)

AP – Access Point (dostopovna točka)

SSID – System Set IDentification (identifikator nabora storitev)

Izdalo: MNZ RS, Policija / Priprava: GPU, UKP / Oblikovanje: Alten, d.o.o. / Tisk: Simpro, d.o.o. / Naklada: 500 izvodov / September 2006