NAVODILO ZA UPORABO STORITEV DOSTOPA DO INTERNETA

T-2 vsakemu naročniku storitev dostopa do interneta namesti in da v uporabo uporabniško napravo različnih vrst in tipov. Tip naprave lahko naročnik razbere iz označbe na napravi, priloženega navodila o uporabi naprave ali dokumenta, ki ga ob vzpostavitvi storitve in predaji opreme prejme od T-2 strokovnjaka.

Uporabniška naprava je namenjena tudi nudenju drugih storitev T-2 kot sta stacionarna telefonija in internetna televizija. Sledimo temu, da je uporabniška izkušnja ne glede na vrsto ali tip uporabniške naprave enaka oz. primerljiva.

Na uporabniške vmesnike uporabniške naprave prehoda se priklapljajo druge uporabniške naprave, ki so lahko:

- uporabnikovi terminali (računalniki…);
- uporabnikove komunikacijske naprave (usmerjevalniki, WLAN dostopne točke, požarne pregrade, …);
- naprave, ki jih zagotovi T-2 za potrebe drugih storitev (STB, telefonski prehodi, …).

Za uporabo drugih uporabniških naprav in uporabo drugih storitev imajo naročniki in uporabniki na razpolago druga navodila za uporabo.

Uporabniška naprava je in ostaja v lasti T-2 kot ponudnika storitve. Naročniki in drugi uporabniki so dolžni z njimi ravnati v skladu z navodili iz dokumenta “Osnovna navodila”, ki so na razpolago za vsak tip uporabniške naprave in navodili iz Splošnih pogojev uporabe storitev.

Uporabniške naprave vrste premoščevalnik

Navodilo se uporablja za naslednje tipe premoščevalnikov: SVL100D-LR, SV2M101, SVM104, SV2M104, SV2M108, LevelOne, Raisecom in Milan.

Storitev internetnega dostopa z IPv4 naslovom

V okviru storitve internetnega dostopa z IPv4 naslovom, T-2 na omrežni strani omrežnega prehoda dodeli dva javna IPv4 naslova. IPv4 naslov je lahko:

- dinamičen in ga ponudnik storitve dodeli omrežnemu prehodu ob vključitvi in resetu naprave oz. ga lahko menja vsakih 24 ur;
- statičen in ga ponudnik storitve dodeli naročniku na podlagi naročila dodatne storitve.

Uporabniške naprave vrste omrežni prehod IAD

Navodilo se uporablja za omrežne prehode Innbox V45, Innbox V50U, Innbox V60U, Innbox F60 in Innbox G64.

Storitev internetnega dostopa z IPv4 naslovom

V okviru storitve internetnega dostopa z IPv4 naslovom, T-2 na omrežni strani omrežnega prehoda dodeli en javni IPv4 naslov. IPv4 naslov je lahko:

- dinamičen in ga ponudnik storitve dodeli omrežnemu prehodu ob vključitvi in resetu naprave oz. ga menja vsakih 24 ur;
- statičen in ga ponudnik storitve dodeli naročniku na podlagi naročila dodatne storitve

Na strani omrežja uporabnika oz. na uporabnikovi napravi lahko uporabnik izbira med:

- statičnim privatnim naslavljanjem z uporabo nabora privatnih IPv4 naslovov od 192.168.64.2 do 192.168.64.99 (prehod 192.168.64.1, maska 255.255.255.0);
- dinamičnim privatnim naslavljanjem in uporabo nabora privatnih IPv4 naslovov od 192.168.64.100 do 192.168.64.200;
- DMZ cona (demilitarizirana cona) ja razpoložljiva v privatnem IPv4 naslovnem prostoru od 192.168.64.2 do 192.168.64.99 (prehod 192.168.64.1, maska 255.255.255.0). Možnost aktivacije / deaktivacije DMZ in izbora DMZ privatnega IPv4 naslova je na https://horizont.t-2.net (Nastavitve – Mrežna oprema – Izberite opremo) ali z zahtevo podano preko klicnega centra T-2 (telefonska številka: 064 064 064).

Brezžično WLAN omrežje

Brezžično WLAN omrežje deluje na frekvenci 2.4 GHz in podpira protokole v skladu s standardi 802.11 b/g/n. Prednastavljene vrednosti parametrov za dostop do WLAN omrežja so unikatne in navedene na oznaki na hrbtni strani omrežnega prehoda (ime omrežja oz. SSID, ključ, WPS PIN). Naročnik lahko vrednosti parametrov za dostop do WLAN omrežja spremeni na uporabniškem portalu https://horizont.t-2.net v rubriki nastavitve mrežne opreme.

Varnost pred grožnjami na internetu

V okviru storitve dostopa do interneta so naročniki izpostavljeni grožnjam kot so:

- virusi, ki napadajo računalnike in mobilne terminale ter škodijo njihovemu delovanju, delovanju aplikacij in ogrožajo podatke na njih;
- trojanski konji, zaradi katerih postanejo računalniki in mobilni terminali ranljivi in izpostavljeni napadom;
- aktivnosti črnih hekerjev (phishing), ki želijo pridobiti vaša uporabniška imena in gesla z lažnimi elektronskimi sporočili, lažnimi spletnimi stranmi in drugimi škodljivimi orodji;
- druge vrste škodljive programske opreme (malware) in škodljive aktivnosti hekerjev.

Zaradi zgoraj navedenih razlogov vam svetujemo in priporočamo, da svoje privatno računalniško omrežje, računalnike in drugo uporabniško ali programsko opremo ter svoje podatke zaščitite:

- s protivirusno zaščito, ki naj se redno posodablja;
- s požarnimi pregradami na posameznih računalnikih, mobilnih napravah in drugi uporabniški opremi;
- z namestitvijo samostojne požarne pregrade ali požarne pregrade v komunikacijski omrežni opremi v primeru večjega računalniškega omrežja;
- z rednim posodabljanjem operacijskih sistemov računalnikov, mobilnih terminalov in druge uporabniške opreme, saj se s tem odpravljajo odkrite varnostne ranljivosti (varnostne luknje),

- s pazljivim ravnanjem pri odpiranju nepoznanih in nepričakovanih elektronskih sporočil ter pazljivostjo pri odpiranju spletnih strani, ki jih obiskujete. Bodite pozorni, da se vselej izogibate posredovanju uporabniških imen, gesel, PIN kod in drugih identifikacijskih podatkov dokler niste popolnoma prepričani, da bodo ustrezno uporabljeni in ne bodo zlorabljeni.

Podan spisek groženj in varnostnih ukrepov ni popoln, saj se vsak dan pojavljajo nove grožnje. Priporočamo vam, da se z njimi seznanjate in se na to temo redno izobražujete.

Več informacij je na voljo na spletnem mestu www.varninainternetu.si.

Omejitev odgovornosti T-2

T-2 kot ponudnik storitev ni odgovoren za škodo, ki bi vam lahko kot naročniku ali uporabniku storitve dostopa do interneta nastala zaradi realizacije groženj.

Ponudniki storitev smo v skladu z Zakonom o elektronskih komunikacijah zavezani spoštovati načelo nevtralnosti interneta, po katerem se vsak internetni promet na javnem komunikacijskem omrežju obravnava enakovredno, to je neodvisno od vsebine, aplikacij, storitev, naprav, virov in ciljev komunikacije.

Četudi kot ponudnik storitev v posameznih primerih omogočimo prevajanje javnih naslovov IP v privatne in obratno (t.i. network address translation – NAT funkcija), je ta namenjena učinkoviti rabi javnega naslovnega prostora in ne zagotavljanju zaščite naročnikov in uporabnikov storitev dostopa do interneta pred grožnjami globalnega interneta.