VIRTUAALSED PRIVAATVÕRGUD - INFOAJASTU ASUTUSTE SELGROOG

Kirjutas Isahiir
Wednesday, 16 November 2005

Virtuaalsed privaatvõrgud – infoajastu asutuste selgroog

Globaliseerumine ja sellega kaasnev elektroonse andmeside üha laienev kasutuselevõtt on tänapäeval protsessid, millega võib iseloomustada praktiliselt kõiki inimtegevuse valdkondi. Tavakasutajale ja reatöötajale tähendab see eelkõige võrguühenduse (üha enam püsiühenduse) olemasolu töökohal ning selle kasutamist kõige mitmekesisematel viisidel ja erinevateks eesmärkideks, millest üks on ka tööalase info vahetus ja hankimine.

Tihti jäetakse tähele panemata jätkuva võrgustumisega kaasnevad ohud, selle varjuküljed. Siinkohal ei hakata rääkima mitmesugustest viirustest, trooja hobustest, rämpspostist ja muudest uue aja väärnähtustest. Neist olulisem on tõdemus, et Internet (aga just sellega samastatakse tihti globaliseerumine ja ülemaailmne andmeside) on juba oma olemuselt ja ülesehituselt ebaturvaline, kuna algselt, võrgustiku loomisjärgus ei osatud laivõrgu turberiske vaadelda kui ohtu, mille vastu kindlustatust tuleks võrgu projekteerimisel arvestada.

Nagu teada, tekkis Internet akadeemilises keskkonnas ning areneb siiani suures osas vaba (tasuta levitatava ja kõigile parandusteks avatud) tarkvara toel, mille puhul on oluline info kättesaadavus — et kõigile soovijatele oleks ressursid avatud ja kasutatavad. Tänapäeval aga kasutatakse Internetti üha rohkem kommertsiaalseks ja ametialaseks suhtluseks, kus kiire infovahetuse kõrval (mida Internet kahtlemata võimaldab) on oluline ka andmete terviklus (muutusi tohivad teha vaid need, kellel selleks volitused) ja konfidentsiaalsus (mitte igaüks ei pea saama kõike vaadata). Ainuüksi Interneti tavavahendeid kasutades ei saa võrgus liikuva info turvalisust täielikult tagada, küll aga on see võimalik, kui kasutada ideoloogiat, mida tänapäeval tuntakse virtuaalse privaatvõrgu nime all.

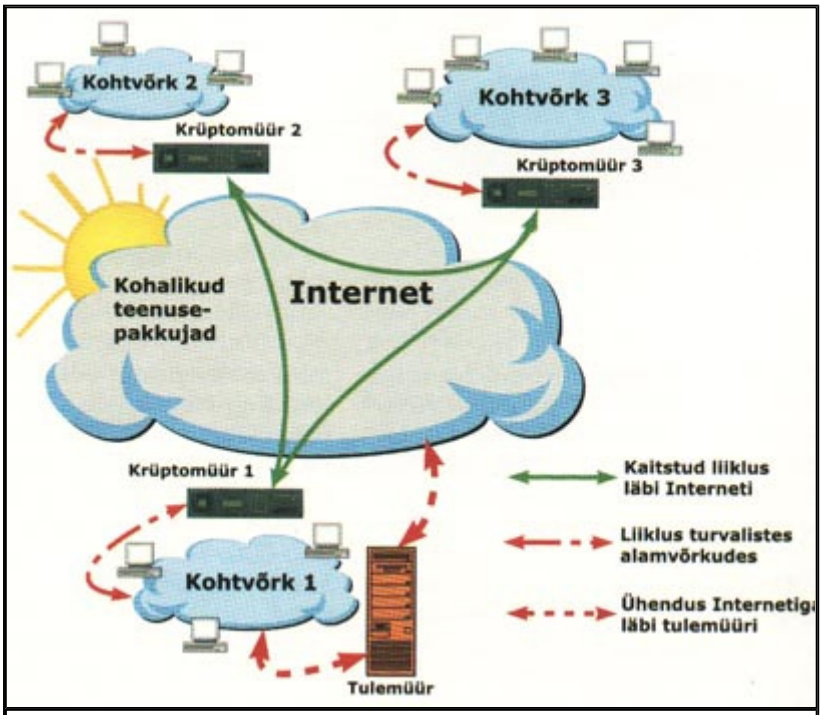
Virtuaalsed privaatvõrgud

Infoühiskonna üheks tunnuseks on infot vahetavate subjektide (töötajate) sõltumatus geograafilisest asukohast — töötegemine ei ole enam seotud büroo asukohaga, vaid on piiratud üksnes organisatsiooni liikmeks olemisega. Virtuaalsete privaatvõrkude (VPN, Virtual Private Network) mõiste pole üheselt defineeritud, kuid enamasti mõeldakse selle all ühe organisatsiooni sisest andmesidevõrku, kus mitu (tihti geograafiliselt eraldatud) alamvõrku (näiteks eri büroodes) on ühendatud loogiliseks tervikuks. Paneme tähele, et mõistes iseenesest ei sisaldu kasutatava andmesidekanali liik. Tõepoolest, VPN–e on võimalik luua kõige erinevamaid meediume kasutades, alates büroode vahele füüsiliste liinide väljaehitamisest kuni üldlevinud Interneti kasutamiseni, nende vahele jääb veel Frame Relay jms poolprivaatsete kanalite kasutamine.

Kanalist sõltumata kerkib kasutajate ette turbe tagamise küsimus — kuna VPN–e kasutatakse enamasti asutusesiseselt, liigub neis ka konfidentsiaalset infot, mida volitamata vaatajatele näidata ei soovita. Seetõttu lisatakse VPN–i mõistele tihti ka turvalisus — ühendus eri alamvõrkude vahel peab olema realiseeritud selliselt, et andmete konfidentsiaalsus oleks tagatud. Kuna Interneti–ühendus on tänapäeval laialt levinud ja kättesaadav ning suuremas osas organisatsioonides niikuinii andmesideks kasutatav, võib loomulikult tekkida küsimus, kas poleks võimalik sidet just selle kanali kaudu korraldada.

Internetis liikuvad andmepaketid on võrgu ehituse eripärade tõttu loetavad (ja muudetavad) ka kõigile teistele võrgukasutajatele, kuid ebaturvalisuse probleemi saab elimineerida — keegi pole ju öelnud, et avalikus võrgus ühest alamvõrgust teise liikuvad andmed ja paketid peaksid tingimata olema needsamad, mis ühest otspunktist lähtuvad ja lõpuks teise, turvalises alamvõrgus asuvasse arvutisse peavad jõudma. Vahepeal, kui andmed on avalikus võrgus, võiks nad salastada ja nõnda võõraste silmade eest

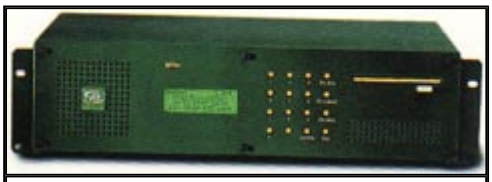
varjata, ning hiljem (kui ohtu enam pole ja andmed jõuavad taas sisevõrku) tagasi esialgsele kujule viia. Seni, kuni säilib pakettide terviklus (st nende endi sisu ei muudeta), võib nendega ju teostada igasuguseid teisendusi, mille hulka mahub ka (de) krüpteerimine.



Joonis 1. Turvaline virtuaalne privaatvõrk

Turvatud liiklus

Joonisel 1 on esitatud põhimõtteline virtuaalse privaatvõrgu skeem, kus andmed liiguvad üle avaliku Interneti, kuid liiklus on kaitstud (krüpteeritud). Süsteemi kuulub kolm alamvõrku (näiteks kolm bürood), millest igaüks on Internetti ühendatud läbi erilise võrguseadme, krüptomüüri. Seadme nimi tuleneb tema põhifunktsioonist — krüptomüüri ülesandeks on krüpteerida „oma" sisevõrgust teistesse võrkudesse liikuvaid pakette (ning dekrüpteerida teistest sisevõrkudest pärinevaid andmeid ja edastada nad seejärel oma sisevõrku). Krüptomüüril on kaks võrguliidest — neist üks ühendatud sisevõrku ja teine Internetti.



Joonis 2. Krüptomüür

Tsentraalne haldus

Põhimõtted

Virtuaalse privaatvõrgu joonist vaadates võib tekkida küsimus süsteemi halduse ja administreerimise korralduse kohta, kuna haldusprotseduure pole näidatud. Krüptomüürid iseenesest on projekteeritud töötama ka missioonikriitilistes keskkondades (st töökindlus on olulisim krüptomüürile ja tervele VPN–süsteemile esitatav nõue), kuid keegi peab nad enne töölehakkamist ka paigaldama. Samuti on oluline küsimus, kuidas lahendada krüptomüüride konfigureerimine edasise töö käigus — nt kui süsteemi lisandub uus alamvõrk ja selle ees olev krüptomüür, peab teiste krüptomüürideni jõudma info sellest, et on võimalik suhtlus uue partneriga, samas

peavad seda infot saama edastada ainult need, kellel selleks volitused olemas (et ei algaks andmevahetus süsteemiväliste, teistele organisatsioonidele kuuluvate krüptomüüridega ega toimuks infoleket).

Turul olevate VPN–toodete projekteerimisel on kasutatud mitmeid erinevaid lähenemisi. Leidub tooteid, kus krüptomüüride administreerimine ja sätete muutmine on võimalik ainult kohapeal, näiteks krüptomüüri esiküljel oleva juhtpaneeli või välise kuvari ja klaviatuuri vahendusel. Selliste süsteemide administreerimine on suhteliselt vaevarikas, sest ka väiksemate konfiguratsioonimuudatuste korral tuleb konfiguratsiooni muuta kõigis krüptomüürides kohapeal eraldi, mis halduskulusid loomulikult suurendab.

Teistsugust lähenemist kasutab nn tsentraalne haldusmudel, kus põhirõhk VPN–i käigushoidmisel on viidud süsteemi administraatorile, kes vastutab kogu privaatvõrgu töö eest ja kelle töökoht asub reeglina organisatsiooni peakorteris. Seal töötatakse välja nii turvapoliitika kui ka selle rakendamise põhimõtted, mis seejärel spetsiaalseid turvalisi protokolle kasutades edastatakse üle Interneti kõigile krüptomüüridele. Need võtavad edastatud uue konfiguratsiooni automaatselt kasutusele ning tihti ei pruugi isegi krüptomüüri ülem, rääkimata lõppkasutajatest, mingisugust muutust süsteemi töös üldse märgata. Üheks tsentraalset mudelit kasutavaks VPN–süsteemiks on Eestis, Küberneetika AS–is välja töötatud Privador.

Mõneti on tsentraalse mudeli loomisel ajaloolised põhjused — seda tüüpi VPN–ide loomise initsiaatorid ning esimesed kliendid olid näiteks Eestis mitmed suured riigiasutused, kelle puhul on loomulik üleriigilise turvalise võrgu vajadus, samas saab määratleda asutuse peakorteri, kust kogu võrku administreeritakse. Teisalt on tsentraalse haldusmudeli kasutamine mõttekas igasuguste mitmest alamvõrgust koosnevate VPN–ide puhul, kuna tihti ei leidu kohapeal (igas võrgusõlmes) piisavalt ekspertteadmisi keerulisema krüptomüüri konfigureerimiseks ja süsteemi haldamiseks. Sel juhul tuleks ühel (või mitmel, kui soovitakse end kindlustada nt inimese erinevatel põhjusel puudumise ja selle põhjustatud süsteemi töövõimetuse vastu) inimesel läbida suhteliselt spetsialiseeritud ja kallis koolitus, mis loomulikult süsteemi kogumaksumust (TCO — Total Cost of Ownership) tõstaks.

Tsentraalse haldusmudeli puhul võib rääkida kahte liiki administraatoritest — kohapealsete krüptomüüride administraatorid (ülemad) ja kogu süsteemi töö eest vastutav süsteemi administraator (süsteemiülem). Harukontoreid kaitsvate krüptomüüride ülematele pole VPN–i kasutuselevõtul eraldi koolitust vaja, kuna nende ülesanded on suhteliselt piiratud, lihtsad ja detailses kasutajajuhendis kirjeldatud. Igapäevast hooldust krüptomüürid ei vaja ja, nagu öeldud, konfigureerib neid peakorteris töötav süsteemi administraator, kasutades selleks spetsiaalseid juhtprogramme.

Ka tsentraalset haldusmudelit kasutava süsteemi tõrgete korral ei pea krüptomüüri ülem ise neid lahendama hakkama, seda enam, et tal lahendamiseks vajalikud ekspertteadmised tihti puuduvad. Spetsiaalse teavitusskeemi alusel edastatakse krüptomüürides töö jooksul tekkivad tõrketeated nii krüptomüüri kontrollmoodulile (kust krüptomüüri administraator neid LCD–paneeli vahendusel ka lugeda saab) kui ka süsteemiülema kasutatavatele juhtprogrammidele, mis võivad omakorda kriitilisemad teated lühisõnumina edastada süsteemiülema või vastava krüptomüüri administraatori meiliaadressile, peilerile vms. Sel viisil kindlustatakse, et info süsteemi tööd ohustavatest kriitilistest probleemidest jõuab õigeaegselt võtmeisikuteni. Krüptomüüridele teadete edastamine on tihtipeale vaid informatiivne, kuna enamasti reageerib neile süsteemiadministraator, kuid kasulik võib see olla nt võrguhäirete puhul, kui teated ei jõua alusvõrgu probleemide tõttu krüptomüürist kaugemale. Sel juhul võivad tõrketeated olla isegi esimeseks märgiks võrgutõrgetest — kuid probleemide kiire avastamine ja kõrvaldamine tagab alusvõrgu ja VPN–i häireteta toimimise, mis on ju organisatsiooni eduka töö aluseks.

Tulevikuväljavaated

VPN–ide populaarsusele maailmas ennustavad erialaväljaanded plahvatuslikku kasvu — arvatakse, et praegu sadades miljonites dollarites mõõdetav turumaht kasvab mõne

aasta jooksul mitme(kümne) miljardini. Paljudes asutustes ei peeta VPN–i soetamist tänapäeval veel taskukohaseks, kuid infovahetuse ja organisatsioonide arenedes (kasvades) tundub VPN paljudele mõne aasta pärast sama loomulik nagu tänapäeval Interneti–ühendus. Kindlasti tasuks süsteemi valimisel pöörata tähelepanu selle turvalisusele (sealhulgas töökindlusele) ja kasutamismugavusele.

http:// jaanus.kase@cyber.ee /
http://www.cyber.ee/infoturve/

Kasutatud kirjandus:

"Virtuaalsed privaatvõrgud – infoajastu asutuste selgroog" *Jaanus Kase "AM" 8/1999*

KOMMENTAARID

Viimati uuendatud (Thursday, 24 November 2005)