Arvutivõrgud lihtsamaks ja turvalisemaks

25 aastat tagasi - 09.11.2001 Autor: AM

Autor: **Hurmi Jürjens**

Uute sidetehnoloogiate kasutuselevõtt on võimaldanud paremini ära kasutada vaskkaabli- ja kaabeltelevisoonivõrke, mille tulemusena saab järjest enam kasutajaid avaliku võrguühenduse - kas sealt siis informatsiooni hankimiseks, meelelahutuseks või ka erinevate reaalajas toimivate sidelahenduste väljatöötamiseks. Interneti areng ning sellega kaasnev suundumus avatud süsteemide ja võrkude laiendamisele kombinatsioonis IP (Internet Protocol) ja Ethernet (lokaalvõrk) populaarsusega loob uusi võimalusi nii juurdepääsuteenuse pakkujatele, ettevõtetele oma spetsiifiliste rakenduste käivitamiseks kui ka tavalisele koduarvuti(võrgu) kasutajale. Seetõttu on kohtvõrgu (LAN) lahendused saamas ilmseks võistlejaks laivõrguteenustele, seda nii juurdepääsusõlmede kui ka tuumikvõrgu osas.

Juurdepääsuteenuse pakkujad on turule toonud lisaks siiani tavaks olnud püsiühendusele ka ADSL -tehnoloogial põhinevaid pakette, mis avardab klientide võimalusi saada kvaliteetset juurdepääsuteenust pea kõikjal, kus on võimalik kasutada digitaaltelefonijaamade teenuseid.
Äriettevõtted kasutavadki juba võimalust luua üha enam elektroonilisi kasutajaliideseid ja siduda neid Internetikeskkonnaga paremaks klientide teenindamiseks ja oma äripartneritega suhtlemiseks. Lisaks avaneb võimalus odavate ja kiirete, kõikjal kättesaadavate võrguteenuste abil peale ettevõtte allüksuste lokaalvõrkude sidumise anda oma töötajatele võimalus töötada kodus. Ka koduarvuti kasutaja saab nüüd senisest enam võimalusi Internetikeskkonnas toimetamiseks, kuna juurdepääsuteenuste hinnad langevad, teisalt suureneb ka Internetikeskkonnas kättesaadavate teenuste hulk.

Interneti kriitiliseks parameetriks on aga tema avatus. Näiteks pankades ja teistes suuremates ettevõtetes kasutatavad arvutisüsteemid ja -võrgud on juba sünnipäraselt turvalised võrgurünnete suhtes ning teenuste kvaliteedi tase võrdub kliendi sooviga selle eest maksta. Kuid tavatarbija ja väiksema firma jaoks eksisteerib tihti probleem, kui soovitakse soetada oma arvutivõrgu turvalisuse tagamiseks vajaminevaid vahendeid, kuna nende kõrge hind on tihtipeale ületanud võimalusi investeerida. Teisalt seab kiirete võrguühenduste astronoomiline juurdekasv uued nõuded lairiba turvalahendustele - lahendustele,

mis võimaldaksid muuta avatud Interneti kasutamise sama turvaliseks kui seda on suure ettevõtte kohtvõrk, samal ajal mitte pärssides kiirete võrguteenuste kättesaadavust.

Lairibainternetiteenuste turvalisus

Lairibainternetiteenus (broadband Internet) on kõigile vabalt kättesaadav. Seetõttu tuleb avalikku võrku ühendatavais süsteemides väga hoolikalt läbi mõelda kasutatavad kaitsemehhanismid, kuna üha sagedamini juhtub, et häkker avastatakse koduarvutit ründamast või märgatakse mõnel suuremal veebilehel kellegi poolt omavoliliselt tehtud muudatusi.

Lairibavõrgus tuleb niisiis leida lahendus kahele põhilisele turvalisust tagavale ülesandele: suurendada häkkerikindlust ning luua turvalisi ühendusi teiste võrkudega üle avaliku IP võrgu.

Nagu näeme juurdelisatud skeemilt, saab häkker rünnata iga kaitsetut avalikku võrku ühendatud arvutit - ning seda kahel põhilisel põhjusel. Nendeks põhjusteks on esmalt valdava osa arvutite "alati sisselülitatud" olek, mis annab häkkerile võimaluse rünnata ajal, mil teda parasjagu jälgida ja segada ei saa, ning teiseks staatilise IP olemasolu, mis võimaldab juba kord rünnatud masinat taas uuesti kasutada. Peab märkima, et ka kõige odavamate ADSL /kaablipakettide kasutajad, kui nad oma arvutit iga sessiooni lõpul välja ei lülita, on pea samasuguses ohus kui kallimate pakettidega kaasaantavate staatiliste IP aadresside kasutajad, kuna ka sel juhul säilib sessiooni algul kliendile eraldatud IP -aadress muutumatuna.

Häkkerid on varustatud lihtsalt kasutatavate vahenditega, mille abil nad skaneerivad mitmeid kordi päevas kogu Internetis avalikke IP aadresse eesmärgiga avastada kaitseta arvuteid. Paljud avalikku võrku ühendatud arvutite kasutajad on märganud, et nende arvutit üritatakse väljastpoolt uurida. Eriti ohtlik on selline tegevus operatsioonisüsteemi Windows kasutajatele juhul, kui arvutis aktiveerida failide ja printeri jagamine. Kuid ka teiste operatsioonisüsteemide kasutajad pole päriselt priid ohust, mis kaasneb arvuti ühendamisega avalikku võrku. Kuigi kodukasutajate probleemid seonduvad tavaliselt ühe Internetiühendust vajava arvutiga, siis viimasel ajal on paljudes kodudes tekkimas vajadus lisaks juurde ühendada ka teine või ka kolmas arvuti, loomulikult koos võimalusega pääsuks Internetti.

Kuidas oma arvutit kaitsta?

Seega on tekkimas olukord, kus peale avalikku võrku ühendamise turvalisuse tagamise nõutakse juba ka kodudes pea samasuguseid teenuseid nagu siiani väiksemates äriettevõtetes - lokaalvõrgus peaks töötama DHCP , NAT ja VPN teenused ja tuleks kontrollida ka lokaalvõrgust väljuvat ja sinna sisenevat IP - liiklust.

Äriettevõtetes kasutatakse üldiselt kaht põhilist lahendust: kas paigaldatakse oma lokaalvõrku vastava tarkvaraga spetsiaalne serverarvuti ja usaldatakse välisühenduse turvalisuse tagamine teenusepakkujale või ostetakse kogu lokaalvõrgu kaitseks riistvaraline seade, nn "tulemüür". Seega võib tulemüür olla nii riist- kui ka tarkvaraline seade.

Esimene võimalus on odavam, kuid seda vaid juhul, kui kasutatakse vabatarkvara (nt Linux) rakendusi. Kui minna välja mõne kommertsplatvormi valikule, võib sarnane lahendus olla mitu korda kallim. Lisaks eeldab tarkvara kasutamine selle head tundmist, milliseid omadusi pole kahjuks paljudel ettevõtjatel. Seega tuleks palgata inimene, kes kogu sellel keerulisel masinavärgil silma/kätt peal hoiaks.

Teine võimalus seevastu moodustab nii väiksema ettevõtte kui ka suure allüksuste arvuga suurema ettevõtte jaoks küllalt mahuka investeeringu, ulatudes sadadesse tuhandetesse kroonidesse.
Kodukasutaja valikud sarnanevad ettevõtja omadega, kui vajadus sunnib kokku ühendama mitut arvutit. Ka siin on tavaliselt ikkagi tarvis abi või nõu küsida tuttavalt "patsiga poisilt", aga kuidas toimida, kui pole sellist tuttavat ?

Mida on selles valdkonnas juba tehtud

Senini põhiliselt kasutatavad lahendused on olnud mõeldud põhiliselt väikese läbilaskvusega välisühenduste turvamiseks, baseerudes arvutitarkvaral (põhiliselt PC/ UNIX lahendused) ning mille puudused välisühenduste kiiruste tõusuga üha enam ilmsiks tulevad. Põhilisteks tarkvaralise turva lahendusplatvormi puudusteks on esiteks tema orienteeritus tarkvaraliselt läbiviidavale pakett-töötlusele ja riistvara ettevalmistatus küll arvutustehete sooritamiseks, kuid mitte võrguliikluse otsetöötluseks, teiseks selle installatsiooni mitmeastmelisusest tulenev keerukus, mis hõlmab lisaks ka erinevaisse valdkondadesse siirduvaid hankeid ja head orienteeritust erinevate riist- ja tarkvaraliste koosluste valikul, ning kolmandaks - tulemusena saadava keeruka süsteemi omandamisest kergesti tekkida võiv petlik turvatunne. Lisaks operatsioonisüsteemile, mida selline süsteem oma tööks vajab, on ka riistvaralise poole pealt selle nõrgaks kohaks just selle mehaaniline konstruktsioon - hulgaliselt ventilaatoreid, kõvaketas, ülekuumenev protsessor - kõik sellised tegurid kokku ei moodusta arvutisüsteemi

osana just selle tugevaimat lüli.

Internetis opereerivad suuremad teenusepakkujad ja ka geograafiliselt hajusat struktuurvõrku kasutavad ettevõtted on seetõttu siiani kombineerinud erinevatest seadmetest nn "tulemüüri-sandvitše", kasutades kriitilisemates liikluskanalites võimalike ummistuse tekkimise vältimiseks mitut tarkvaralist paralleelselt toimivat tulemüüri (mille tootjad ja müüjad rõhuvad omakorda turvalisuse tõusule, kuna tõepoolest ühe sellises komplektis oleva lahenduse tõrge ei vii rivist välja kogu süsteemi, vaid tekitab vastava jõudluse languse antud seadmele langenud koormuse ulatuses) mida mõnikord tavatsetakse nimetada ka krüptomüüriks. Sellegipoolest on ka sellisel lahendusel märkimisväärseid puudusi, kuna ta nõuab palju füüsilist ruumi, tarvitab palju energiat (põhiliselt küll Eesti Energia poolt toodetavat) ja kütab serveriruumi - seega järgmine investeering tuleb planeerida uue konditsioneeri soetamiseks.

Samuti ei saa unustada ka süsteemiadministraatori energiakulu kogu selle kaskaadi konfigureerimiseks. Kokkuvõttes on tegemist küllalt tülika, kindlasti kallivõitu ja mitte seejuures alati kuigi turvalise lahendusega.

Nõuded teise generatsiooni turvalahendustele

Teise põlvkonna turvalahendused lahendavad valdava osa eelloetletud probleemidest. Esiteks on nad riistvarapõhised lahendused - seega ei ole häkkeril võimalik kasutada süsteemi sissemurdmiseks operatsioonisüsteemile omaseid nõrku kohti; teiseks - kogu vajalik teenuste skaala on integreeritav ühte seadmesse; kolmandaks võimaldavad sellised lahendused kiirusi alates 10 Mbps kuni 1,2 Gbps, seejuures ilma vajaduseta mitme erineva seadme paralleelühenduseks; ja neljandaks - süsteemi konfigureerimine on lihtsam ja mugavam, ja mis põhiline - aega kulub selleks minimaalselt, kuna juba tehases on riistvarasse kõik vajalikud võimalused sisse ehitatud.

Riistvarapõhise turvalahenduse moodustab spetsiaalselt antud eesmärgiga konstrueeritud ASIC -põhine (ASIC - Application Specific Integrated Circuit - rakendusspetsiifiline integraalskeem) rakendus, integreerides endasse andmeliiklust inspekteeriva tulemüüri, VPN koos krüpteerimisega ja liikluse ribalaiuse kontrolli funktsionaalsuse koos uue generatsiooni lairibarakenduste keskkonnaga. Eelnimetatud riistvara südameks on kiire RISC protsessor ja rakendus sisaldab kaitset kõigi põhiliste rünnete vastu. Samuti on samas seadmes lisaks tulemüürile olemas nii NAT (Network Address Translation), PAT (Port Address Translation) teenused, mis varjavad välisvõrgu eest mittemarsruuditavaid IP -aadresse, kui ka DHCP server sisevõrgu tarvis. Samuti

on süsteem suuteline välisvõrgus kas PPPoE või DHCP abil töötama ilma staatilise võrguaadressita.

Eelkirjeldatud teise põlvkonna lahendus on säästlikum eelmise põlvkonna lahendusest, ei tekita töötamisel müra, selles puuduvad mehaaniliselt liikuvad osad ja traditsiooniline operatsioonisüsteem, mis kokku kahandab arvutisüsteemide keerukuseastet ja lisab töökindlust. Kuid peamine on siiski, et uue põlvkonna turvalahenduste tootjad on arvestanud ka kodukasutajate ja väikefirmade vajadustega, mistõttu nüüdsest saab võimalikuks ka märgatavalt väiksemate kulutustega soetada professionaalse süsteemiga ühilduv lahendus, mis oma soodsa hinna ja kvaliteedi suhte tõttu on kogumas üha enam poolehoidjaid. Näiteks võib tuua joonisel kujutatud struktuurskeemi, millel kujutatakse süsteemi, kus ettevõtte peakontor ja tema allüksused on ühendatud ühtsesse loogilisse lokaalvõrku VPN krüpteeritud kanalite vahendusel.

Seega - enne laivõrguga ühendamist tuleks kriitilise pilguga vaadata üle oma arvutisüsteem välisühenduse poolelt või siis paluda seda teha asjatundjatel. Ning kui selgub, et hetkeseis jätab soovida enamat, on soovitav valida asjatundjatega konsulteerides oma võimalustele ja vajadustele sobivaim lahendus. Tasub teada, et uue põlvkonna riistvaralised võimalused rahuldavad kindlasti ka kõige nõudlikuma kliendi soovid.

- Lahendused

- Turvalisus
- Võrguseadmed