TULEMÜÜR -KAITSE TEISTE ARVELT

Kirjutas Isahiir
Wednesday, 16 November 2005

Tulemüürikaitse teiste arvelt

Tulemüürid on koduste alarmsüsteemide infotehnoloogilised analoogid. Analoogiline on ka olukord nende kasutamisel: samuti nagu enamikus kodudest puuduvad korralikud häiresüsteemid, pole ka suurel osal ettevõtete infosüsteemidest korralikku tulemüürikaitset. Kui inimesed oma koduses eelarves ei raatsi turvasüsteemidele kuigivõrd suuri kulutusi teha, pole ime, et sama põhimõtet järgitakse ka firmatasandil.

Firmajuhtide tõrksus oma infosüsteemides korralikke turvameetmeid rakendada põhineb enamasti vaid kergete kõhklustega varjutatud illusioonil, et häkkerid nende süsteeme ei ähvarda. Seetõttu püütakse andmeturbesse investeerida nii vähe kui võimalik, varustades oma süsteemid ainult vältimatute ja kõige silmnähtavamaid riske välistavate kaitsevahenditega.

Loomulikult eksisteerib valdkondi, kus turvanõuded on sedavõrd kõrged, et nende arvelt koonerdamine lihtsalt ei tule kõne alla: militaarsüsteemid, pangad jms. Siiski eelistab enamus nn tavaorganisatsioone andmekaitsele võimalikult vähe kulutada, pidades investeeringuid sellesse valdkonda tarbetuks raiskamiseks. Nii mõnegi finantsdirektori veenmine andmeturbe-alaste kulutuste tegemiseks tundub juba ette kaotatud lahinguna. Seda vaatamata faktile, et seoses Interneti, sisevõrgu ja kommuteeritavate liinide üha laiema levikuga on oht häkkerite rünnakute ohvriks langeda tunduvalt kasvanud ning et sellised rünnakud võivad põhjustada ettevõttele märkimisväärset materiaalset kahju.

Soovitud tulemüürikaitse saavutamiseks on siiski olemas ka nn kõrvalteid. Kuna tulemüüride uus põlvkond on kõrge multifunktsionaalsusega ning pakub seega käegakatsutavat ärilist kasu, on väga võimalik tulemüürikaitse saavutamine mõne muu funktsiooni arvelt või vähemalt kulutuste jagamine mõne teise osakonnaga. Tulemüürikomplektide uusim tüüp (mis ennustuste kohaselt moodustab 2001. aastaks 80% kogu tulemüüride turust) pakub laialdast multifunktsionaalsust samas rakenduses.

Moodne tulemüürikomplekt pakub mitte ainult tulemüürikaitset, vaid ka virtuaalset privaatvõrku (VPN) harukontorite ja kaugtööks, samuti andmete krüpteerimist, autentimist ja sertifitseerimist, IP paketihaldust (nt kõne- ja videoedastus läbi Interneti), veebipöörduse haldust ja aruandlust, vahendeid juurdepääsu tõkestamiseks teatud veebilehtedele (pornograafia, rassism, jututoad jne). Üks funktsioonidest on ka aadresside transleerimine, mis väldib vajadust hankida igale arvutile oma IP-aadress, kui eesmärk on üksnes ligipääs veebile.

Kõik nimetatud funktsioonid võivad ülihästi teenida firma, selle mingi osakonna, äristruktuuri või spetsiifilise projekti huve, sealhulgas ärilist kasu tuues. Seega võib neid hankida ka kellegi/millegi muu kui IT- või andmeturbe kulude arvelt.

Harukontorite virtuaalseid privaatvõrke võib harukontorite või haru- ja peakontori vahelise suhtlemise turvamise seisukohalt finantseerida näiteks side-eelarve või harukontorite endi arvelt; kaugkasutajate virtuaalseid privaatvõrke näiteks müügiosakonna arvelt kui meetmeid mobiilse müügitegevuse arendamiseks ja turvalise andmesidega kindlustamiseks; andmete krüpteerimist võib käsitada osana e-kaubanduse programmide vältimatutest turvameetmetest ning finantseerida seda spetsiaalsest e-kaubanduse eelarvest või rahandusosakonna poolt esitatud nõudmisena finantseelarvest.

Tulemüürikomplektide uus generatsioon võib pakkuda kõiki eelmainitud omadusi ning lisaks tasuta tulemüürikaitset. Pealegi väheneb oluliselt, mõnekümne tuhande kroonini, tulemüürikomplektide hind. Kuna paljud kirjeldatud funktsioonidest pakuvad mitte niivõrd otsest ärikasumit, kuivõrd võimalusi kulutuste oluliseks vähendamiseks, muutub nende ühendamine tulemüüriteenustega ahvatlevaks pakkumiseks.

Virtuaalsed privaatvõrgud

Virtuaalsed privaatvõrgud (VPN) võimaldavad Interneti kaudu turvaliselt andmeid saata ja vastu võtta. Sellised võrgud on vajalikud juhtudel, kui firmal on püsivat sidet vajavaid allüksusi mitmes eri paigas või kui tekib vajadus

regulaarse andmete vahetamise järele eri asukohtade vahel. Kuna Internetti saab kasutada kohalike sideliinide kaudu, pakuvad VPN-id olulist säästu võrreldes rendiliinide kasutamisel. Üldreeglina pakuvad VPN-id seda suuremat säästu, mida suuremad on vahemaad.

Andmete Interneti kaudu saatmise odavus tähendab ka seda, et andmesideühendus, mis varem ei õigustanud rendiliini hankimist, on nüüd VPN -keskkonnas turvaliselt hallatav.

Kaugkasutaja juurdepääs

Kui süsteemi andmebaasi kasutab sissehelistamise teel hulk kaugkasutajaid, tähendab see ka hulka modemeid, mida on vaja toetada ja hallata ning mille ühenduste eest kasutajad peavad maksma vastavalt kehtivatele tariifidele.

Kasutades tulemüüriga kaasnevaid VPN-võimalusi, mis lubavad saata informatsiooni Interneti kaudu kohalike kõnetariifide alusel, pole enam vaja teha kulutusi eelnimetatud modemipankade haldamiseks ning tänu kohalike tariifide kasutamisele on võimalik vähendada kulutusi telefonsidele.

Kaugkasutaja VPN võimaldab info turvalist edastamist. Kaugpöörduses kasutatakse *de facto* standardit PPTP (*Point-To-Point Tunnelling Protocol*) Windows 95-le. See loob turvalise tunneli, mille kaudu krüpteeritud informatsioon avalikus võrgus ohutult liigub. Sihtpunkti (nt peakontori) tulemüür loob VPN-i ja moodustab turvalise keskkonna, milles krüpteeritud andmed kahe võrgupunkti vahel liiguvad. Kaugkasutaja VPN välistab ka probleemi, kus liialt palju kaugpöördusega kasutajaid koormaks üle piiratud arvu modemeid, ning seeläbi tõuseb taas süsteemi kasutajasõbralikkus.

Kui kaugpöördusega kasutajaid on optimaalne hulk, teeb kaugkasutaja VPN rakendamisest saadav halduskulude kokkuhoid õige pea tasa tulemüüri muretsemiseks tehtud kulutused.

Autentimine ja sertifitseerimine

Tulemüür pakub ka autentimis- ja sertifitseerimisteenuseid, mis välistavad modeminumbrite kaugsideks väljajagamisega seotud riskid. Olles kindel, et kaugkasutajad pääsevad süsteemi ainult turvatud teid mööda, on võimalik kaugkasutajate hulga suurendamise teel tõsta ettevõtte tootlikkust.

Näiteks on kaugkasutuse teel võimalik kiiremini vastu võtta ja töödelda tellimusi. Kliendid võivad esitada oma tellimused interaktiivselt otse süsteemi, mis kahandab müügitööle tehtavaid kulutusi.

Andmete krüpteerimine

Pole mägede taga aeg, mil lõviosa kaubandusest toimub elektrooniliste kanalite kaudu. Juba praegu kasutatakse massiliselt firmadevahelist elektronposti, tellimuste esitamist meili teel, interaktiivseid kaubakatalooge jms. Peamine nõue firmadevahelises suhtlemises on see, et sõnum jõuaks kohale. Siiski vajab teatud osa informatsiooni, näiteks rahalised vms firma seisukohalt konfidentsiaalsed andmed, garanteeritud turvet, mida pakub andmete krüpteerimine. Paljud tulemüürikomplektid on võimelised krüpteerima kogu väljamineva elektronposti ning töötlema sissetulevaid krüpteeritud teateid. Seega, kui olukord nõuab konfidentsiaalsust, on tulemüür võimeline seda pakkuma.

Kuna krüpteerimine on protsessorile küllaltki koormav tegevus, pakub tulemüürikomplekt võimalust teha seda autonoomses serveris, selle asemel et ekspluateerida niigi koormatud võrguserverit.

IP paketihaldus

Interneti-ühenduse olemasolu toob endaga kaasa vajaduse või soovi terve rea võrguprotokolli (IP) lisavahendite järele. Näiteks võib tunduda ahvatlevana soov edastada kõnet või videopilti Interneti kaudu ning sel teel vähendada firma kulutusi ja tõsta produktiivsust.

Kõneedastus Interneti kaudu pakub näiteks kokkuhoiuvõimalusi tänu Interneti-ühenduse maksustamisele kohalike tariifide alusel; videopildi edastus (nt videokonverentsid) hoiab kokku reisimisele kuluvat raha ja aega;

kolleegidevahelise suhtlemise hõlbustumine mõjub positiivselt firma tootlikkusele. Samuti toob kasu tavapärase videokonverentsi asendamine Interneti kaudu peetavaga.

Samas tekib mure, et igasugused säästud kulutustes annulleerib vajadus kogu olemasoleva võrgu täiendamise järele, et see saaks hakkama küllaltki intensiivsete erikoormustega, mida toob kaasa mainitud rakenduste kasutamine.

Tulemüürikomplekt pakub vahendeid ja võimalusi IP-teenuste seireks ja haldamiseks ning ülevaadet nende mõjudest võrgu tööle. Saadud informatsioon võimaldab hallata olemasolevaid IP-rakendusi ning stabiliseerida võrgu tööd.

Näiteks, kui ilmneb, et rakendus kõne edastamiseks läbi Interneti aeglustab teatud kellaaegadel liigselt võrgu tööd, võib mainitud ajavahemikes kasutada traditsioonilisi telefoniliine ning muul ajal Interneti-ühendust. Selline lahendus võib olla kasulikum kui kogu võrgu täiendamine toimetulekuks kõikuva koormusega.

Aadresside transleerimine

Olukorras, kus veel kogu firma pole ühendatud veebiga, võib ilmneda pisut häiriv asjaolu. Nimelt antakse kõik IP-aadressid välja ühtse numbrisüsteemi IANA (*Internet Assigned Number Authority*) põhjal ning seda teeb enamikul juhtudest Interneti teenusepakkuja. See tähendab, et võrgu laiendamise vm muutuste korral osutuvad olemasolevad IP-aadressid vigasteks ning need tuleb käsitsi ümber muuta. See omakorda tähendab häireid võrgu töös (ning võimalikke kulutusi), kuna muutuste tegemine võtab aega: isegi väiksema võrgu korral terve õhtu, suurema võrgu korral on see aga võimalik ainult võrgu marsruuteritega jagamise teel ning võib röövida mitu õhtut (nädalavahetust).

Seegi probleem on lahendatav tulemüürikomplekti abiga, mis pakub võrguaadresside transleerimiseks välja vahendi NAT (*Network Address Translation*), mida tuntakse ka IP-teeskluse nime all. Olemasolev IP-aadress säilitatakse võrgus ning tulemüürikomplekt transleerib sisenevad ja väljuvad andmevood registreeritud aadressidele. See meetod pakub ka lisaturvet, kuna kasutajate IP-aadressid pole sel juhul Internetis nähtavad.

Juurdepääsu tõkestamine teatud veebilehtedele

Kui firma avab oma töötajatele juurdepääsu veebile, avanevad sealjuures võimalused ka Interneti kasutamiseks ja sealt materjalide allalaadimiseks kõlvatutel eesmärkidel (nt porno, rassism). Vastutustundetute töötajate poolt korralikele kolleegidele nähtavakstehtud või isegi edastatud kõlvatu info võib negatiivselt mõjutada kollektiivi tööõhkkonda ning firmadel lasub moraalne vastutus kaitsta oma töötajaid vastavate saitide kahjuliku mõju eest. Asjal võib olla ka juriidilisi tagajärgi, näiteks USA-s on juba olemas pretsedente, kus töötajad on oma tööandjad selliste intsidentidega seoses moraalse kahju põhjustamise eest kohtusse kaevanud.

Oluline vahend taoliste kuritarvituste ärahoidmiseks on ametijuhendid. Kuid samavõrra tähtsad on veebilehtede blokeerimise vahendid, mis võimaldavad ligipääsu tõkestamist teatud sisuga saitidele ning põhinevad regulaarselt värskendatavatel veebiandmebaasidel. Selliste tõkete ülesseadmine annab töötajatele märku tööandja sallimatusest veebi kuritarvitamise suhtes ning ennetab võimalikke kulukaid juriidilisi vaidlusi. Seda tüübi veebilehtede blokeerimisvahendid sisalduvad paljudes tulemüürikomplektides.

„Mittetöise" kasutuse tõkestamine

Pole harvad juhud, mil töötajad surfivad tööajal Internetis nn mittetöistel eesmärkidel. Gartner Groupi andmetel hõlmab selline „oma lõbuks" Interneti kasutamine enam kui 20% kogu veebis veedetud ajast. See tähendab tööaja kadu ja sidekulude suurenemist, samuti koormab võrke ning aeglustab seega arvutisüsteemide tööd.

Veebihalduse vahendid, mida pakuvad ka tulemüürikomplektid, võivad Interneti kasutamist selleltki seisukohalt kontrollida ja reguleerida. Näiteks on

võimalik talletada andmed iga töötaja poolt külastatud veebiaadresside kohta, samuti blokeerida juurdepääsu nn mittetöistele saitidele, hoides sel moel ära veebi ebaotstarbeka kasutamise.

Lisaks töö produktiivsuse tõusule pakuvad taolised veebihalduse programmid veebikasutuse andmete fikseerimise kaudu süsteemihalduritele võimalust vastavate regulatsiooniabinõude ja -vahendite plaanimiseks.

Kokkuvõtteks võib öelda, et uut tüüpi tulemüürikomplektid on teinud revolutsiooni andmeturbes. Vanad tulemüürid olid üleliia kulukad, neid oli keeruline installida ja kasutada, mis omakorda põhjustas vajaduse kallite spetsialistikonsultatsioonide järele. Tänased tulemüürikomplektid on tunduvalt odavamad (riistvara ja tarkvara kokku alates 50 tuhandest kroonist) ega vaja spetsiaalseid lisaseadmeid. Neid on lihtne installida ja kasutada, nad on multifunktsionaalsed, pakkudes peale tulemüürikaitse ka mitmeid lisateenuseid.

Kõik see ei tähenda mööndusteid tegemist andmeturbe arvelt. Pigem on multifunktsionaalsuse taga tõik, et tulemüüridki järgivad nüüdisaja üldist tehnoloogilist trendi, pakkudes väiksemate kulutuste eest rohkem funktsionaalsust.

Kui teil ei õnnestu oma firma juhtkonda veenda maksma tulemüürikaitse eest, pakkuge kaasaegset tulemüürikomplekti mõnel muul eelpoolkirjeldatud eesmärgil ning saategi tulemüürikomplekti pealekauba, mõne muu funktsiooni arvelt kinnimakstuna.

Kasutatud materjalid:

"Tulemüürikaitse teiste arvelt" *Ian Kilpatrick* "AM" 4/1999

KOMMENTAARID

Viimati uuendatud (Thursday, 24 November 2005)