MIKS SISEVÕRGUD ON LOOMULT EBATURVALISED

Kirjutas Isahiir
Wednesday, 16 November 2005

Miks sisevõrgud on loomult ebaturvalised

Arvutivõrkude turvaohtudele pühendatakse tänapäeval palju tähelepanu. Enamasti keskendutakse väljastpoolt lähtuvale ohule, mis paistab kasvavat. Näiteks tunnistasid hiljaaegu toimunud küsitlusele vastanutest 20%, et nende ettevõtte võrku oli viimase 12 kuu jooksul rünnatud Internetist (Computer Weekly, 17. September 1998). Kuna üldiselt peetakse tõenäoliseks, et enamust ründekatseid ei märgata, peab väliste häkkerite poolt rünnatavate võrkude arv olema tegelikkuses palju suurem.

Ehkki välised ründed annavad põhjust muretsemiseks, tuleb samuti meeles pidada, et enamus andmetele volitamata ligipääsusid, andmete varguseid ja kahju tekitamisi lähtub ettevõtte seest. FBI statistika viitab, et 70% turvariskidest võrkudele on firmasisest päritolu.

Nagu väljastpoolt tulevad ründed, nii muutuvad ka ettevõttesisesed ohud turvalisusele üha tavalisemaks. Nad tekivad, kui ettevõtte töötajad ületavad oma volituste piire lootuses rahalisele kasule või üritavad saada informatsiooni, mida neil pole õigust omada. Mõned töötajad tahavad lihtsalt pahandusi põhjustada, mõned aga kolleegide palku teada. Rahulolematud töötajad püüavad hankida konfidentsiaalset infot, et seda müüa või avalikustada.

Inimesed võivad ettevõtte süsteemides kolamist alustada lihtsast uudishimust; kaugemale minnakse pärast vahelejäämisohu puudumise avastamist. Mõned inimesed soovivad sihilikult kahju tekitada, kuid tõenäoliselt moodustavad nad vähemuse. Ehkki süsteemi kokkukukkumine torkab silma ja avalikkus peab teda seetõttu peamiseks puuduliku turvalisuse tagajärjeks, on enamikel juhtudest motiiviks siiski lihtsalt soov saada informatsiooni.

Haavatavad võrgud

Ettevõtte sisevõrgud on eriti õrnad seestpoolt lähtuvate rünnete suhtes. Riski ulatusest on nii selle teema juures kui mujalgi keeruline selgust saada, kuna firmad ei soovi tunnistada oma võrkude turvalisust ebapiisavaks. Samas pole kahtlust, et juhtumid, mis avalikkuse ette jõuavad, kujutavad endast vaid jäämäe pealmist osa.

Sisevõrkude haavatavusel on mitmeid põhjusi. Sisevõrk luuakse ettevõtte andmestiku parema kättesaadavuse jaoks; viimane toob kasu äriliselt, kuid ühtlasi seab andmed ohtu.

Enamgi, sisevõrgud luuakse algul sageli otstarbeks, kus turvalisus pole oluline, näiteks sisemiste infolehtede ja töötajaskonna käsiraamatute levitamiseks. Alles sisevõrgu peamise kasutuseesmärgi muutumisel selgub, et oma olemuselt turvamata võrk loob ettevõtte jaoks riske.

Sisevõrgud ja nendega seotud süsteemid on tavaliselt loodud tasapinnalise ettevõttestruktuuri jaoks. Seetõttu pole neisse planeeritud volituste süsteemi, mis oli traditsioonilise suurarvutitel põhineva hierarhilise süsteemi oluline osa.

Lisaks on oluliselt kasvanud töötajaskonna võime turvaprobleeme põhjustada. Kümme aastat tagasi oli ettevõtte töötajaskonnas ainult väga väike osa töötajaid, kes osanuks selle turvet murda. Tänapäeva PC–maailmas võivad kasutaja oskused olla võrreldavad IT–osakonna oskustega, eriti veebimaterjalide kättesaamisel.

Töötajad tõenäoliselt teavad, kuidas kasutada ettevõtte inforessursse. Häkker väljastpoolt võib süsteemis kulutada tunde, enne kui leiab midagi kasulikku, kuid oma töötaja jõuab hetkega kõige tundlikuma infoni.

Sisevõrkudel on teatavaid loomuomaseid nõrkusi. Traditsioonilisse süsteemi pääses suheldes serveriga, mis autentis kasutajat põhjalikult ja jälgis ligipääsu andmetele. Sisevõrkudes on teisiti, kui just pole kasutusele võetud erilisi meetmeid. Ettevõtte töötajad võivad seega olla palju anonüümsemad oma võrgutegevuses, ükskõik kas siis töötades kohapeal, kasutades püsiliini või helistades süsteemi sisse.

Kõikjal ühtse TCP/IP–protokolli kasutamine muudab rünnet üritaval töötajal lihtsamaks süsteemis orienteerumise ja võrguliikluse jälgimise.

Tähtsaim nõue

Sisevõrgu turvalisuse lahendamine nõuab turvateadlikku lähenemist, mis väljendub sobiva tarkvara ja riistvara kasutuselevõtus. Üks esimesi samme on tagada, et turvalisust käsitletakse tähtsaima nõudena — see jäetakse sisevõrkude kasutuselevõtul sageli tegemata.

Oluline on teha teatavaks töötajaskonnale, et volituste piire rikkuv tegevus on lubamatu. Selline hoiatamine aitab juba ise ründeid ära hoida, pannes töötajaid tajuma vahelejäämisega seotud võimalikke tagajärgi. Ähvardusi tuleb kinnitada ka tegudega, kui vajalik. Samuti peab turvalisus kuuluma automaatselt arvestatavate asjade hulka, kui ükskõik millist informatsiooni sisevõrku kättesaadavaks tehakse.

Oluline on ka määrata andmeturbe eest vastutav isik või isikud. See isik ei tohiks olla IT –osakonnast vaid mõnest teisest, näiteks finantsosakonnast. Vajalik on see mitmeti. Esiteks, süsteemi tundmine võib teha *status quo* IT–töötajate jaoks lihtsamini vastuvõetavaks. Teiseks, suurem tähelepanu turvalisusele võib IT–projektide käivitamist aeglustada ja IT–osakonnal võib seetõttu tekkida huvide konflikt. Kolmandaks, IT–personalil on paremini kui teistel võimalik volitamatult süsteemi pääseda ja sõltumatu järelvalve on seetõttu soovitatav.

Tulemüür

Kui ülalloetletud nõuded on täidetud, on paras aeg valida tulemüürisüsteem kui riskide vähendamise vahend. Tulemüüri üks põhifunktsioone on erinevate volitustasemete loomine sisevõrgu eri osadele, kuna teatud informatsioonitüübid kujutavad endast ettevõtte jaoks väärtusi ja neid tuleb sellena käsitleda. Näiteks võib tuua finantsinfo, tooteuuringud ja tootearenduse, palganduse ja personaliküsimused.

Uue põlvkonna mitmeotstarbeliste tulemüüride populaarsus kasvab ja need on ideaalseks sisevõrgu turvalisuse lahenduseks. Nad sisaldavad nii tarkvaralisi kui ka riistvaralisi elemente, mistõttu neid võiks nimetada tulemüürikomplektideks. Nende laiadele kasutusvõimalustele tulemüürina lisanduvad madal hind ja seadistuse ning kasutamise lihtsus, mis muudavad nad sobivateks kasutamisel võrgu sisemistes riskipunktides. Sageli pakuvad nad lisaks häid kaugjuhtimise võimalusi ja aruannete koostamise vahendeid.

Tüüpiliselt võimaldavad tulemüürikomplektid määrata ja kontrollida erinevate kasutajagruppide volitusi sisevõrgu eri osades. Näiteks müügiosakonnal võib olla lubatud kasutada ainult osa informatsioonist või ainult kindlal ajavahemikul. Eriti tundlikke andmeid käsitlevatel osakondadel võivad lisaks olla oma sisemised tulemüürid.

Sellised mitmeotstarbelised komplektid võivad samuti pakkuda kaugkasutajate autentimise ja virtuaalvõrkude (VPN) vahendeid. Samuti võivad nad pakkuda ulatuslikke jälgimise ja aruandluse võimalusi. Valima peaks tulemüürirakenduse, mis on paindlik ja seadistatav vastavalt kohapealsetele vajadustele ja mis võimaldab erinevate harukontorite või sisemiste turvaelementide juhtimist ühest keskprogrammist.

Tulemüüri funktsioonide hulgas peaks üldiselt olema teavitamine kõikide turvanõuete rikkumiskatsete puhul, teenuse blokeerimine ründe avastamisel, valitud portide või teenuste jälgimine vajadusel koos juurdepääsu keelamisega, logifailide salvestamine

kahtlasest tegevusest teatamiseks. Kokkuvõttes peaks tulemüür andma sisevõrgus toimuva kohta reaalajas ülevaate igal ajahetkel.

Tõeline kasu

Kaasaegsed tulemüürikomplektid võivad anda väärtusliku panuse sisevõrgu turvalisusesse. Nende hinnad algavad 50 tuhandest kroonist (selles sisaldub ka riistvara). Tulemüüride vastu tunnevad kasvavat huvi ettevõtted, kes otsivad hinnalt sobivat võimalust oma sisevõrgu organiseerimiseks ja kontrollimiseks. Gartner Groupi ennustuse kohaselt esindavad sedasorti tulemüürikomplektid aastaks 2001 80% kõigist tulemüüridest.

Siiski peab arvestama, et sisevõrkudest tuleb arvestatavat kasu ainult juhul, kui nad moodustavad osa ettevõtte struktuurist. Turvalisus on struktuurilise lähenemise keskne osa ja tuleb seetõttu sisevõrku sisse planeerida algusest peale.

Kasutatud kirjandus:
"Miks sisevõrgud on loomult ebaturvalised" "AM" 1/1999 *Ian Kilpatrick*

"Miks sisevõrgud on loomult ebaturvalised" "AM" 1/1999

KOMMENTAARID

Viimati uuendatud (Thursday, 24 November 2005)