Kogu tõde Interneti turvalisusest

1. oktoober 2005 - 0:53 Autor: Jaan Vare

Andmeturbefirma Symantec tutvustas septembris raportit „Ohud Interneti turvalisusele", millest selgub, et rünnete hulk ja kiirus on kasvanud, nendele reageeritakse aeglaselt ning enamus auklikest programmidest on seotud Internetiga. Samast raportist saab ka teada, et vabavaralised ja palju kiidetud Mozillal põhinevad brauserid nagu Firefox on kaks korda ebaturvalisemad kui palju kirutud Microsoft Internet Explorer .

Traditsiooniline poolaasta raport on üks olulisemaid ja põhjalikemaid sellesarnaseid dokumente, mida Interneti turvalisuse kohta koostatakse. Symantec teeb seda alates 2002. aasta jaanuarist.

Robotid ründavad

Seekordne Symantec Internet Security Threat Report puudutab ajavahemikku jaanuar-juuli 2005 ning sai avalikuks eelmisel kuul. Kõige kõmulisem ja rohkem avalikkust puudutanud sõnum käis loomulikult Mozilla brauserite kohta ja ütles, et need on palju rohkem haavatavamad kui Internet Explorer , mida Microsoft sageli lapib.

Raportist saab aga teada muudki huvitavat, mh ka seda, et küberkurikaelad on muutnud oma profiili ega korralda enam nii massiliselt suuri, multifunktsionaalseid rünnakuid, vaid spetsialiseeruvad kindlale valdkonnale. Oluline on ka, et kurja ei tehta enam lihtsalt uudishimust, mis oli varem valdav rünnakute motiiv, vaid kasu saamise eesmärgil - olgu selleks siis identiteedivargus, väljapressimine või pettus.

Kui reaalses maailmas on raha väljapressimine levinud eraisikutelt, siis e-maailmas ähvardavad kurjategijad e-firmasid: „Kui sa meile ei maksa, siis korraldame sinu vastu denial-of-service tüüpi rünnaku". Identiteedivargused on e-kuritegelike tüüpide juures ühed kõige populaarsemad. Konfidentsiaalse informatsiooni - krediitkaardinumbrid, e-panga koodid jne - saamiseks korraldatud rünnakud moodustasid TOP 50 rünnakute nimekirjas 74%. See on viiendiku võrra rohkem kui pool aastat varem.

Ka viiruste arv kasvas kuue kuuga hüppeliselt. Symantec tuvastas vaadeldud perioodil 10 866 uut Win32 viirust ja ussi; eelmise aasta teises pooles oli see arv ainult 7360. Kui aga minna ajas veel 6 kuud tagasi, on kasv koguni 142% (4496 uut viirust ja ussi).

Uurides programmide haavatavust, leidis Symantec 1862 uut turvaauku, mis on kõigi aegade suurim number. Kõikidest aukudest 49% olid väga ohtlikud, 59% kõikidest probleemidest seotud aga Interneti-programmidega (109% rohkem kui aasta varem).

Robotite ehk botide korraldatud rünnakud olid ühed kiiremini kasvavad: poole aastaga avastati 10 352 boti päevas, mis on üle kahe korra rohkem kui 2004. aasta detsembris. Symantec on seisukohal, et robotite suurenenud aktiivsus on otseselt põhjustanud ka DoS-rünnete suurenemist.

Robotid on programmid, mis paigaldatakse kasutaja teadmata tema arvutisse ning neid hakkab Interneti teel juhtima kurjategija. Pahatahtlike robotitega nakatunud arvutitest luuakse bot network ehk robotite võrk, mille abil saab korraldada laiaulatuslikke DoS-rünakuid. Sedasorti rünnakud on väga levinud ja muutuvad järjest populaarsemaks: alates jaanuarist kasvas DoS-rünnete hulk 680% ja küündis 927 rünnakuni päevas. Hoolimata aga DoS-rünnakute massilisusest, on suurte firmade hulgas kannatanuid väga vähe.

Mobiil pole turvaline

Ka mobiilsed seadmed ei ole küberkurjategijate eest kaitstud. Tänavu kevadel avastati esimene MMS-i teel leviv ussviirus Commwarrior, mis ohustab põhimõtteliselt kõiki, kellel on multimeediasõnumeid toetav mobiiltelefon. Kuigi esialgu on mobiilsete seadmete vastu suunatud rünnakud ja viirused veel harvad, ennustab Symantec nende kiiret kasvu. Esialgu on aga suurimas ohus nutitelefonide kasutajad. Võrreldes arvutikasutajatega ei pea nad siiski eriti muretsema.

Üle poole kirjadest spämm

Üks suuremaid kasvuprotsente oli seotud spämmiga. Selle aasta esimese kuue kuuga avastas Symantec 1,04 miljardit e-kirja, millega püüti arvutikasutajat petta (phishing). Eelmise aasta juulist detsembrini oli vastav arv 546 miljonit ehk 90% vähem. Vaadeldud perioodil saadeti seega iga päev 5,7 miljonit petukirja, mis tähendab omakorda, et iga 125. saadetud e-kiri oli phishingu katse. Üleüldine spämmi hulk tavakirjadest moodustas 61%, millest omakorda 51% oli pärit USA-st, kus on teadupärast karmid spämmi saatmist reguleerivad seadused.

Ründajad kiiremad kui kaitsjad

Symantec uuris välja, et turvaaukudele reageerisid kräkkerid mitu korda kiiremini kui programmide tootjad. Pärast turvaprobleemi avastamist lõid kurjategijad seda turvaauku ära kasutava viiruse või ussi keskmiselt kuue päevaga. Programmide tootjad aga reageerisid veaparandusega keskmiselt 54 päeva hiljem. See tähendab, et kräkkeritele jäi 48 päeva muretuks tegutsemiseks.

Kasutajate ainus pääsetee oli loota enda arukusele, kuid seegi pole alati võimalik. Teine võimalus oli loota, et ettevõtte administraator kõrvaldab ise tootjapoolse vea. Osalt tänu programmide tootjate aeglasele reageerimisele kasvas nt DoS-rünnakute arv poole aastaga 679%. Huvitaval kombel oli kõige rohkem rünnatud objektiks haridussektor. Sellele järgnesid väikeettevõtete arvutivõrgud.

USA ründab

Syamntec uuris ka, millistest riikidest kõige rohkem rünnakuid pärines. Kuna ründaja tegelikku asukohta on keeruline (ja mõnikord ka võimatu) tuvastada, on tabelis toodud just maad, kus asus arvuti, millest rünnak alguse sai. Ründaja tegelik asukoht võib sellest kõvasti erineda, sest enamasti püüavad pahategijad oma asukohta varjata ning kasutavad mitmeid erinevaid (ja eri maades asuvaid) süsteeme. Nii võib ründaja asuda ise Hiinas ja New Yorkis asuva süsteemi ründeks kasutada hoopis Lõuna-Korea arvutit.

USA osakaal rünnakute päritolumaade hulgas on 33%, mis on 3% rohkem kui eelmise aasta lõpus ja 4% vähem kui 2004. aasta alguses. USA populaarsuse põhjuseks peab Symantec sealsete lairibaühenduste suurt hulka, ning ennustab, et tulevikus kasvab USA osakaal veelgi.

Haridus on lemmik

Vaadeldes ründeobjekte valdkonniti, selgub, et kõige rohkem pakuvad kräkkeritele huvi haridusasutused, mida rünnati kaks korda rohkem kui finantsasutusi. Selle põhjuseks on koolide ja instituutide laiad võrgud ning kasutajate suur arv.

Teisele kohale jäänud väikeettevõtted on ohustatud aga oma piiratud võimaluste tõttu: neil pole piisavalt vahendeid, et oma võrku turvata. Praegu kolmandale kohale platseerunud finantsasutustele ennustab Symantec kiiret rünnakute arvu kasvu, sest selle valdkonna ettevõtteid rünnatakse peamiselt tulusaamise eesmärgil ning just see muutub üha enam kräkkerite motiiviks.

Kogu tõde Mozillast

Kui varasematel perioodidel on olnud peamised rünnakuobjektid võrku kaitsvad ressursid, nagu tulemüürid, serverid jt, siis viimasel ajal on oluliselt suurenenud brauserite ründamine ja nende kaudu süsteemidesse tungimine.

Enim turvaprobleeme kõikidest vaadeldud veebisirvijatest (MSIE, Mozilla, Opera, KDE Konqueror, Safari) oli Mozilla brauseritega, mille hulka kuulub ka Firefox. Symantec avastas 25 turvaauku, mis on mõnevõrra vähem kui 2004. aasta teisel poolel, mil avastati 32 viga. Sellest 25 turvaprobleemist 18 olid väga tõsised (võrdluseks: 2004. a teisel poolel sai sama hinnangu 14 viga).

Samal ajal oli Microsoft Internet Exploreris 13 turvaauku, mis on võrreldes eelmise vaadeldud perioodiga oluliselt vähem (2004. a juuli-detsember avastati 31 auku). Avastatud 13 august nimetas Symantec tõsiseks 8, mis on kümne võrra vähem kui Mozilla brauserites.

Apple'i brauser Safari oli uuritud veebisirvijatest üks turvalisemaid - avastati ainult kaks turvaviga, mis on sama palju kui eelmisel perioodil. Ühte avastatud aukudest nimetas Symantec kõrge riskiga turvaprobleemiks.

Norrakate Opera, mille litsentsi eest tuli vaadeldud perioodil veel palju raha maksta, pääses tabelisse kuue turvaprobleemiga. See on hea tulemus, arvestades, et 2004. aasta lõpus oli Operas 11 auku. Pooled avastatud vigadest olid väga tõsised, ülejäänud ei kujutanud endast erilist ohtu.

Kokkuvõtvalt leidis Symantec, et viimasel vaadeldud perioodil oli brauseritel vähem tõsiseid turvaauke kui varasematel aastatel. Eriti torkab see silma MS Internet Exploreri puhul, sest Microsoft on astunud mitmeid probleeme ennetavaid samme.

- Lahendused