

Beveiliging op internet verbetert met de dag. Toch zijn veel systemen niet zo goed beveiligd als men zou denken. Een internationaal onderzoeksteam was benieuwd naar de mate van beveiliging van systemen op Internet. De groep ontwikkelde de Bulk Auditing Security Scanner om in een kort tijdsbestek zoveel mogelijk systemen over de hele wereld te kunnen controleren. Onlangs publiceerde het team de resultaten, waaruit we kunnen concluderen dat er in veel gevallen nog veel werk aan de winkel is voordat systemen op Internet écht waterdicht zijn.

Internet Audit project scant netwerklekken

Medio 1998 besloot een groepje onderzoekers uit verschillende landen samen te werken om inzicht te krijgen in het percentage netwerken dat kwetsbaar is voor bekende zwakheden in besturings-systemen en netwerkprogramma-tuur.

Daar waar Farmer eind 1996 een steekproef gebruikte om een

indruk te krijgen van de veiligheid van systemen die aangesloten zijn op het Internet, ging deze groep uit van het auditen van zoveel mogelijk systemen. De aanpak vereiste het schrijven van een programma dat zo snel mogelijk zo veel mogelijk systemen kan ondervragen. Daarnaast was het nodig om op een slimme wijze adressen van systemen te verzamelen. Deze scanner is genaamd Bulk Auditing Security Scanner (BASS). De eerste versie van de BASS-programmatuur bekijkt overigens alleen Unix systemen.

Testen

De ontwikkeling van het programma vergde een aantal teststappen. Zo bleek de programmatuur na het scannen van 18 duizend Israëlische systemen op vier bekende lekken instabiel te zijn. Nadat dit probleem verholpen was, rustten de wetenschappers de scanner uit met

meer testen, waardoor BASS onderzoekt of een systeem kwetsbaar is voor inbraken via achttien bekende beveiligingsgaten in Unix netwerk-programmatuur. BASS kijkt daarbij naar lekken zoals die voorkomen in CGI-webdiensten (onder andere phf, php, wwwcount, glimpse), bij het aanroepen van een remote procedure (rpc.mountd, tooltalk), bind en net nieuws (innnd).

Ondergronds

De ontwikkelaars onderkenden dat het uitvoeren van een dergelijke scan tot een aantal vervelende juridische consequenties kon leiden, ook al zijn er geen geharmoniseerde wetten op het gebied van computercriminaliteit. Het automatisch scannen zou tot vervolging van de onderzoekers kunnen leiden indien de politie overijverig internationale steun zou verlenen. Om die reden werkten ze als kleine groep zonder

Management-summary

Hoe goed zijn systemen op het Internet beveiligd? Die vraag stelde een groep onderzoekers zich eind 1998. Om dit te testen ontwierp de groep de Bulk Auditing Security Scanner. Zij liepen daarmee op de rand van wat wetten en regelgeving in verschillende landen toestaan. Na analyse van de resultaten van het onderzoek publiceerden zij deze medio augustus 1999. Een verslag van de aanpak en een eerste analyse van de resultaten.



enige ruchtbaarheid aan het project te geven.

Om de scan in een betrekkelijk korte tijd te kunnen uitvoeren koos de groep voor het gebruik van een vijftal parallel werkende Unix-systemen, geplaatst in vijf verschillende landen en drie reservesystemen: Israël, Mexico, Rusland, Japan en Brazilië. De systemen waren aangesloten op snelle backbone Internet-verbindingen waardoor ieder BASS-systeem zo'n 250 systemen per minuut kon scannen.

Uitvoering

Op 1 december werd de scan gestart. Nauwlettend hield de groep in de gaten of organisaties waar aan de deur geklopt werd zouden reageren. In de eerste week kregen de wetenschappers slechts enkele reacties, waaronder enkele e-mails en vier tot acht portscans per dag. In de eerste week verkende BASS

systemen van de Amerikaanse overheid, systemen in Canada, Europa en China en een groot aantal kleinere landen. In de tweede week klopte de scanner op de deur van Amerikaanse defensiesystemen (het .mil domein). De onderzoekers constateerden nu een veel hogere activiteit van reacties op de BASS-servers. Daarnaast reageerde iemand door een heel grote stroom pakketten te genereren, wat het Russische netwerk waaraan een van de BASS-servers hing volledig op zijn knieën bracht. In de derde week bleek het Japanse BASS-systeem gekraakt van uit Australië. De inbraak bleek zeer slim uitgevoerd te zijn. De onderzoekers hebben vermoedens dat deze inbraak door een 'professionele' organisatie uitgevoerd is. Op 21 december, na drie weken scannen, waren bijna 36,5 miljoen systemen bezocht. Daarvan bleken 450.000 Unix systemen (1,25 pro-

cent) kwetsbaar. Let wel, de huidige versie van BASS kijkt niet naar lekken in de bezochte Windows- en andere niet-Unix-systemen.

In totaal vond het team 730.213 lekken; sommige systemen kennen dus meerdere lekken. Uit de statistiek wordt duidelijk dat hoe langer het lek bekend was, hoe minder vaak het als aanwezig lek gevonden is.

Waarschuwing

De BASS-scanner bekeek alleen Unix-systemen en slechts achttien bekende lekken. Er zijn veel meer Unix netwerklekken bekend en ook zijn vele andere systemen met niet-Unix-besturingssystemen op Internet aangesloten. Een bekend commercieel product om de veiligheid van netwerksystemen te auditen kijkt naar meer dan 350 mogelijke lekken in Unix- en Windows-systemen.

Het percentage systemen waar eenvoudig op ingebroken kan worden lag volgens de steekproef van Farmer in de buurt van de 35 procent. Uitgaande van marktverhoudingen en de gebruikte lijst met lekken zal het percentage niet goed beschermde, aan Internet gekoppelde systemen nog steeds tien tot twintig procent bedragen.

Tot welke categorie behoren uw systemen? Bij inbraakbescherming van uw huis geldt dat de gelegenheidsinbreker sneller het volgende huis probeert indien uw sloten en beveiliging er degelijk uitzien. Zo ook in cyberspace. Wees alert, installeer nieuwe beveiligingscode zo snel mogelijk en test regelmatig uw systemen met up-to-date audit scanner programmatuur. ■

Literatuur:

'Hoe veilig zijn transacties via het World Wide Web?' Beveiliging jaargang 10, nr. 3, pp. 36-38, 1997

<http://www.securityfocus.com>
The Internet Auditing Project