

onmogelijk de sleutel geheim te houden. Je ziet dan ook dat universiteiten WEP niet gebruiken. Ook al is alle dataverkeer afuis-terbaar als er geen WEP gebruikt wordt, toch kun je nog enigszins toegangscontrole toepassen door bijvoorbeeld alleen bepaalde hardware ethernet-adressen (ofwel bekende wireless kaartjes) toe te laten. Deze beveiliging is ook met weinig moeite te doorbreken, door de toegelaten hardware-adressen af te luisteren en zelf te gaan gebruiken. Uiteindelijk is de enige oplossing voor zulke open netwerken het toepassen van host-security in plaats van netwerk-security, wat zoveel wil zeggen dat het gehele netwerk als niet-vertrouwd wordt aangemerkt. Dat dit niet de meest ideale oplossing is blijkt wel uit het feit dat er slechts één geval bekend is van drive-by spamming, het sturen van hele ladingen ongewenste e-mail via draadloze netwerken. De afzender van deze e-mails is op deze wijze niet meer traceerbaar.

We hebben gezien dat ook het gebruik van WEP niet voldoende beveiliging biedt. Toch is het belangrijk altijd WEP te gebruiken, niet zozeer om het onmogelijk te maken voor inbrekers om op het netwerk te kunnen komen, maar om het moeilijker te maken. Ook juridisch is dat belangrijk: het is toegestaan signalen op te vangen, en wardriving is dus niet strafbaar. Echter, het 'doorbreken van enige beveiliging' is wel strafbaar, zo ook het kraken van WEP dus. Ook al houd je doortastende inbrekers niet tegen met het gebruik van WEP, je maakt het daarmee wel strafbaar.

Oplossingen?

Een WEP-beveiligd draadloos netwerk is in veel gevallen niet veilig genoeg. Er moet dan naar andere oplossingen gezocht worden. Volgend jaar wordt het allemaal wat makkelijker als de IEEE standaard 802.11i klaar is. Hierbij wordt betere versleute-

ling toegepast. Deze nieuwe standaard kan echter pas gebruikt worden na de aanschaf van nieuwe 802.11i-ondersteunende hardware, of het upgraden van de bestaande apparatuur.

De meest veilige oplossing is het draadloze gedeelte van het netwerk te zien als een niet-vertrouwd netwerk en de benodigde maatregelen te nemen. De beveiligingsexperts hebben al jarenlang ervaring met de beveiligingsproblematiek die je krijgt als je twee vertrouwde netwerken verbindt middels een niet-vertrouwd netwerk. Meestal betreft het dan twee vestigingen gekoppeld via het internet, maar je kunt dezelfde principes ook toepassen op de koppeling tussen je laptop en het bedrijfsnetwerk via het draadloze gedeelte.

De oplossing is een Virtual Private Network (VPN). Met technieken als IPsec is het mogelijk alle verkeer te versleutelen en te authenticeren. Het levert extra rompslomp op: op de laptops van de eindgebruikers zullen sleutels moeten worden gezet, net zoals dat bij WEP het geval is. Het base station mag ook niet rechtstreeks aan het interne netwerk gekoppeld worden. Toch is dit momenteel de enige juiste manier om veilig draadloos te netwerken.

En als heel de wereld zijn draadloze netwerken verstandig aansluit (met VPN en een nietszeggende netwerknnaam), dan kunnen de inbrekers zich weer concentreren op nieuwere technologieën. Wat te denken van bluetooth-scannen? •

ir. Walter Belgers

Madison Gurkha

walter@madison-gurkha.com

