Het PAROOL
16-10-2014

'Voor 34 euro kun je al die gegevens onderscheppen'

HERMAN STIL

James Lyne, hoofd beveiliging van internetbedrijf Sophos, fietst door wereldsteden om zo de beveiliging van wifinetwerken te onderzoeken. Deze week is hij in Amsterdam. 'Onveilige praktijken zijn de standaard.'

'De belangrijkste reden dat ik door steden fiets, is dat ik wil aantonen dat er een serieus probleem is. Dat de slechte beveiliging van wifinetwerken al meer dan tien jaar bekend is, betekent niet dat het probleem daarmee is opgelost. Maar mensen reageren niet meer op waarschuwingen. We moeten gebruikers erop wijzen via toegankelijke methodes zoals een fietstocht. Anders wordt hier geen aandacht aan besteed."

Tijdens een rit dinsdag bleek dat 45 procent van de wifinetwerken in de stad niet en nog eens ruim 20 procent niet afdoende is beveiligd. "In de meeste gevallen hebben gebruikers simpelweg geen belangstelling voor het opzetten van hun netwerk, controleren ze daarna niet regelmatig of die instellingen nog wel veilig zijn en veranderen ze hun wachtwoorden en hotspotnamen nooit."

"Vaak zijn wifirouters fabrieksmatig ingesteld op de minste vorm van beveiliging, in plaats van dat ze de gebruiker begeleiden naar de beste vorm van beveiliging. Fabrikanten moeten absoluut verouderde beveiligingsprotocollen als WEP of WPA uit hun apparaten halen, zodat gebruikers ze niet meer kunnen instellen. Er is een bizarre hoeveelheid apparaten beschikbaar dat nog altijd WEP adviseert als beveiligingsstandaard, terwijl al in 2001 is aangetoond dat die beveiliging binnen zestig seconden te kraken is, waarna al het dataverkeer af te vangen is."

Lyne hekelt ook de gebruiksvriendelijkheid van veel routersoftware, die veelal alleen te doorgronden is door doorgewinterde systeembeheerders. "Producenten zouden hun achterhaalde software moeten aanpassen aan hedendaagse standaarden voor software en apps."

Zulke beveiligingsproblemen met wifinetwerken zijn volgens Lyne nog maar het topje van de ijsberg. "Veel oudere routers hebben beveiligingslekken ingebouwd die akelig gemakkelijk geëxploiteerd kunnen worden door kwaadwillenden. Wij mogen dat niet eens aantonen, dat is in strijd met de wet, maar cybercriminelen kunnen ongestoord hun gang gaan. Het zou buitengewoon eenvoudig zijn geweest om tijdens de fietstocht ook te bekijken welke data via wifihotspots worden gedeeld. Om juridi-

sche redenen doen we dat niet. Maar voor 34 euro koop je apparaten waarmee al die gegevens onderschept kunnen worden."

De gedeelde routers van onder meer UPC, KPN en FON, waarmee iedere abonnee ongemerkt ook een deel van zijn internetverbinding openbaar deelt, zijn volgens hem 'redelijk' beveiligd. "Alhoewel in het algemeen de meeste aanbieders zich daarbij concentreren op het beveiligen van hún netwerk, zodat alleen hun abonnees van die gratis hotspots gebruik kunnen maken. Lang niet altijd wordt voldoende gedaan om data te beschermen en om te voorkomen dat andere gebruikers daarnaar snuffelen."

"In het algemeen zijn de beveiligingsstandaarden voor draadloos internet in 2014 vergelijkbaar met die uit 2004. Onveilige praktijken zijn de standaard. Er is een betere draadloze beveiligingsstandaard nodig die het gebruik van publieke wifi in openbare ruimtes veiliger maakt. Zelfs het gedeelde wachtwoord in een restaurant is onveilig, omdat je daarmee toegang kunt krijgen tot het netwerkverkeer van alle gebruikers die er op dat moment gebruik van maken."

Het is sowieso oppassen met openbare wifinetwerken. "Jammer genoeg is het heel lastig echte en nepnetwerken uit elkaar te houden. Iedereen kan een netwerkje opzetten en dat 'Starbucks' noemen. Als je niet zeker weet of je een netwerk kunt vertrouwen en niet kunt navragen wat het officiële netwerk is, log dan helemaal niet in en hou het bij je mobiele netwerk. Als ik onderweg gebruikmaak van een openbaar netwerk, zorg ik er altijd voor dat mijn dataverkeer wordt versleuteld zodat criminelen me niet kunnen bespioneren."