Verhaal van de dag

9 uur geleden

Het wifi-netwerk in treinen van de NS blijkt volstrekt onveilig. Hannes Mühleisen, een lezer van De Correspondent, verzamelde met twee simpele antennes vijf maanden lang data van tienduizenden treinreizigers en kon zo ongemerkt privacygevoelige gegevens achterhalen. De NS doet, ondanks herhaalde waarschuwingen, niets aan het probleem.

De wifi in de trein is volstrekt onveilig (en de NS doet er niets aan)

Maurits Martijn

Correspondent Technologie & Surveillance

Maurits **MARTIJN**

Illustratie: Esther Aarts (voor De Correspondent)

loom, schokkerig, instabiel.

S

Iedereen die weleens gebruikmaakt van de wifi in een NS-trein, weet dat het niet altijd even goed werkt. Soms gaat het twintig minuten goed, soms ben je je de hele treinreis gefrustreerd. Op het ene traject hapert het netwerk continu, op het andere loopt het als een - ja - trein.

Minder bekend is dat 'wifi in de trein' - zoals de netwerken in alle NS-treinen heten - fundamenteel onveilig is. Dáár kun je wel op rekenen. Dat wil zeggen: de netwerken die de NS in zijn treinen gebruikt, zijn nooit versleuteld. Dat wil weer zeggen: data van de wifigebruikers, óók zeer intieme data, zweven onbeschermd en vrijelijk door de lucht.

We weten al langer dat openbare wifinetwerken onveilig zijn. Kwaadwillende hackers kunnen kinderlijk eenvoudig een openbaar netwerk overnemen zonder dat de gebruiker het doorheeft.

Maar dit is een ander verhaal. Bij de wifi in de trein is geen actieve aanval nodig om informatie van en over de gebruikers te achterhalen. Geen hack, geen digitale penetratie of technologische vermomming. Alles wat je nodig hebt is een antenne.

Toen 'wifi in de trein' voorbijkwam

Dat ontdekte Hannes Mühleisen (31). Hij woont op een boot, niet ver ten oosten van Amsterdam Centraal Station. Het spoor ligt zo'n vijfentwintig meter van zijn huis. Een unieke plek, waar de rust van de boten, het water en het groen enkel verstoord wordt door continu voorbij denderende treinen.

De eerste keer dat Mühleisen iets doorkreeg, was in maart van dit jaar. Hij was in de weer met het internet op zijn boot, toen hij rechtsboven in zijn scherm zag dat hij met zijn laptop contact kon maken met het wifinetwerk 'wifi in de trein.' 'Toevallig was ik net met mijn netwerkconfiguratie bezig toen er een intercity met wifi langsreed.'

Hannes Mühleisen in de woonkamer van zijn woonboot, vlakbij station Amsterdam Centraal. Foto: Rob Wetzer

De meeste mensen zouden daar weinig aandacht aan schenken. Niet Mühleisen. Als mannetje van achttien reed hij al rond met een antenne, op zoek naar een wifinetwerk om daar data uit op te slurpen. Toentertijd was dit zogenoemde *'wardriving'* een populair tijdsverdrijf onder nerds. En dus ging er, zegt Mühleisen, 'direct een luikje open' toen hij 'wifi in de trein' voorbij zag komen.

Tot zijn stomme verbazing stroomden de data van de duizenden 'wifi in de trein'-gebruikers zijn woonboot binnen

Mühleisen vroeg zich af of het mogelijk zou zijn om verkeer op te vangen, om 'mee te luisteren' met de apparaten die op 'wifi in de trein' zijn aangesloten. In eerste instantie puur uit nieuwsgierigheid.

Zijn vermoeden was dat het niet zou kunnen. 'De passagiers zitten in een gesloten coupé in een rijdende trein en gebruiken telefoons met niet zoveel vermogen. Daarnaast komen de treinen maar een seconde of twintig langs mijn huis.' En bovendien: zou de NS echt zijn treinreizigers onbeschermd internet aanbieden?

Hij hing twee goedkope antennes die het verkeer van een wifinetwerk kunnen ontvangen naast de deur van zijn woonboot. Om het eventuele dataverkeer om te zetten in begrijpelijke informatie, maakte hij gebruik van opensourcesoftware.

Tot zijn stomme verbazing stroomden de data van de duizenden 'wifi in de trein'-gebruikers zijn woonboot binnen. Informatie over de sites die zij bezochten en de apps die zij gebruikten, de merken van hun smartphones, tablets en laptops en de unieke nummers daarvan.

'Ik was volledig overweldigd door alles wat binnenkwam,' zegt hij.

De gemeten periode was van 11 maart tot 2 augustus 2015. De antennes haalden dag en nacht data binnen. In totaal zijn er 114.558 verschillende Mac-adressen gevonden (unieke nummers van laptops, smartphones, tablets).

De reden dat Mühleisen zo makkelijk mee kon gluren: de wifinetwerken in de trein zijn niet versleuteld. Ze staan open. Wat zoveel betekent als: de data van al die miljoenen gebruikers zweven onbeschermd door de lucht. 'Het netwerk blaast simpelweg alle data uit,' zegt Mühleisen. 'En ik kan ze gewoon uit de lucht plukken.'

Voor de duidelijkheid: Mühleisen verwerkte alleen de metadata van het wifiverkeer, niet de inhoud van de communicatie. Dus wel: dát iemand een bepaalde site bezocht, maar niet wát deze persoon op die site deed. Veel sites en apps maken gebruik van versleuteling, waardoor het onmogelijk is om de inhoud af te luisteren. Facebook bijvoorbeeld. Omdat het NS-wifinetwerk niet versleuteld is kan Mühleisen zien *dat* iemand Facebook gebruikt. Maar doordat de Facebook-app zelf wel versleuteld is, kan hij niet zien wat die persoon op Facebook leest, zegt of doet.

De woonboot van Hannes Mühleisen in de buurt van station Amsterdam Centraal. Foto: Rob Wetzer

Maar niet alle sites en apps zijn versleuteld. Sterker nog: Mühleisen analyseerde dat meer dan de helft van het gebruik van de sites en apps niet versleuteld was. Hij zou mee kunnen kijken met de inhoud ervan, waartoe óók inlogcodes en wachtwoorden, chatsessies en mailwisselingen behoren. Hij heeft het niet gedaan. Maar: 'Als ik zou willen, zou ik hier serieuze rotzooi mee kunnen uithalen .'

Nu was het moment aangebroken om orde te scheppen in de binnenkomende databrij. Voor die volgende stap kwam het best goed uit dat Hannes Mühleisen een gepromoveerd computerwetenschapper is die werkt aan het Amsterdamse onderzoeksinstuut CWI (Centrum Wiskunde & Informatica) en gespecialiseerd is in datamanagement en database-architectuur. Hij bouwde een simpele, elegante database om al die data te ordenen en een krachtige interface om de data te presenteren.

De data van de treinreizigers

Op deze site kun je zien hoe Mühleisen de binnenkomende data heeft geordend en gevisualiseerd.

Het project 'trainwatch' van Hannes Mühleisen

'Je kunt hier zoveel mee doen'

In de vijf maanden dat het project loopt, heeft hij data binnengehaald van 114.558 verschillende apparaten (laptops, smartphones, tablets). Hij heeft data over bijna 10 miljoen pogingen van apparaten om contact te maken met een website of een app.

'Ik heb de unieke nummers van de apparaten, de tijd, de data. Ik weet in welke treinen de apparaten zaten. Als je dit vijf maanden doet, dan leer je de geschiedenis van apparaten en eigenaars kennen. Je kunt hier zoveel mee doen. Stel je voor dat je tien van dit soort antennes op strategische locaties in Nederland neerzet. Dan krijg je een vrij goed beeld van het gedrag van miljoenen Nederlanders.'

'Je kunt er niet aan ontsnappen, de NS geeft de reizigers geen keus'

Als je zo'n enorme bak data hebt, dan kun je ook interessante patronen ontdekken. Bijvoorbeeld dat het dinsdagmiddag om 5 uur het drukst is op de wifinetwerken in de trein. Of dat om 5 uur 's nachts het aandeel Apple-apparaten gemiddeld het laagst is, terwijl het aandeel Samsung-apparaten op dat uur juist op zijn hoogtepunt is. Wat tot de conclusie zou kunnen leiden dat Samsungbezitters grotere nachtdieren zijn dan eigenaars van Apple-apparaten.

In de enorme dataset van Mühleisen zijn ook bevestigingen te vinden van feiten die wij allemaal kennen. Zoals: Apple is verreweg het populairste merk onder treinreizigers. Bijna de helft van de apparaten die in de vijf maanden contact maakten met de wifinetwerken, waren van Apple. Samsung volgt Apple op zeer grote afstand en vanaf nummer drie is het aandeel nogal marginaal.

Illustratie: Esther Aarts

Hartstikke leuk, maar dit mooie laboratorium van het gedrag van de Nederlandse treinreiziger is slechts bijvangst.

Mühleisen wil een punt maken. Hij wil dat de NS zijn reizigers beter gaat beschermen en dat de wifinetwerken standaard versleuteling krijgen. 'Er is geen enkele reden waarom ze hun netwerk niet zouden versleutelen. Dat kunnen ze zo doen. Als jij wifi in de trein gebruikt en je komt langs mijn huis, dan heb ik je. Je kunt er niet aan ontsnappen, de NS geeft reizigers geen keus. '

'Goed weer' is gedefinieerd als: minder dan één uur regen in 24 uur en een maximale temperatuur van meer dan 20 graden. Er zijn 20 willekeurige doordeweekse dagen met 'goed weer' genomen, 20 willekeurige dagen met 'geen goed weer.'

Hoe reageert de NS?

Begin april begon Mühleisen contact op te nemen met de NS. Via Twitter, via e-mail en via de NS-site. Hij vertelde de NS over zijn project en vroeg of zij wilden overwegen encryptie in te stellen. Ik heb alle correspondentie ingezien. De korte versie is: de NS is niet van plan iets aan de beveiliging van de wifinetwerken te doen.

Via Twitter kreeg Mühleisen zelfs te horen dat het niet mogelijk was de beveiliging van de wifi te veranderen. Nadat Mühleisen hen erop wees dat dit pertinent onwaar was, werd hem beloofd dat 'ICT-management' naar zijn vraag zou kijken. Hij heeft nooit meer iets van ICT-management gehoord.

Op een vraag die hij op de NS-site indiende, kreeg hij antwoord van een 'Operationeel Manager Klantenservice': 'Wij stellen het bijzonder op prijs als klanten ideeën aandragen voor verbetering. Uw suggestie over het beveiligen van het Wi-Fi netwerk heb ik inmiddels onder de aandacht gebracht van onze verantwoordelijke afdeling.'

Illustratie: Esther Aarts

Van deze manager of 'de verantwoordelijke afdeling' hoorde hij niets meer.

Toen hij vroeg of hij nog een reactie kon verwachten, ontving hij een e-mail waar Franz Kafka nog een puntje aan kan zuigen:

'U laat weten dat u wilt weten wat er met uw bericht die u heeft doorgegeven gebeurt. Ik kan mij dit voorstellen. Ik geef u graag een uitleg. Mijn collega heeft uw melding van het voorval geregistreerd. Wij nemen dit soort meldingen zeer serieus. Uw melding is daarom naar aanleiding van de registratie van mijn collega doorgegeven aan het verantwoordelijke management. Vervolgens wordt deze besproken. U ontvangt hiervan geen terug koppeling [sic]. Ik hoop, dat u er desondanks vertrouwen in heeft dat wij uw melding zorgvuldig

behandelen.'

In de tussentijd kondigde het bedrijf wél aan dat de 'wifi in de trein' in het derde kwartaal van 2015 sneller én stabieler wordt. Iedere intercity zou met 4G worden uitgerust.

Een voornemen dat valt toe te juichen. Maar het zorgt er ook voor dat meer mensen de netwerken zullen gebruiken, er meer data door de netwerken stromen en de hoeveelheid onbeschermde data toeneemt.

Dus, vroeg Mühleisen: gaan jullie meteen ook de netwerken beter beveiligen?

Nul op het rekest.

Via LinkedIn vond hij het 'Hoofd IT Operations NS' and 'Business Consultant - NS Reizigers IT-Operations'. Beiden reageerden niet op zijn vragen.

Via via kreeg hij het e-mailadres van de persoon bij de NS die verantwoordelijk is voor de wifinetwerken.

Illustratie: Esther Aarts

Geen reactie.

En dat was het moment om de openbaarheid op te zoeken. 'Soms moet je het laten zien om echt een punt te kunnen maken,' zegt Hannes Mühleisen.

Dit blijft hetzelfde

Ik nam ook contact op met de NS. Zijn de wifinetwerken in de treinen al sneller? En worden er beveiligingsmaatregelen genomen? Ook voor een journalist blijkt het niet makkelijk te zijn om contact met het bedrijf te krijgen. Na meerdere mails en belletjes kreeg ik na een week reactie per mail: 'Zodra we hier meer over kunnen vertellen zal NS dat bekendmaken.'

Oké. Ik belde de voorlichter terug en vroeg hem nogmaals of de wifinetwerken beveiligd zouden worden.

Zijn antwoord: 'Ik denk dat dit hetzelfde zal blijven.'

Mocht je de komende tijd van of naar Amsterdam reizen met de trein, via de oostzijde het station binnenrijden (vanuit Maastricht, Utrecht of Nijmegen bijvoorbeeld) óf verlaten (richting, pak 'm beet, Den Haag, Rotterdam, Amersfoort) en gebruikmaken van de wifi, weet dan dat een man met een antenne in een woonboot je data opvangt, opslaat en analyseert.

En dat hij dat met de allerbeste bedoelingen doet.

Met dank aan collega Jesse Frederik, voor de hulp bij de grafieken.

Dit geef je allemaal prijs als je inlogt op een openbaar wifinetwerk

Anderhalf jaar geleden onderzocht ik met een hacker ik de openbare wifi van een paar koffiezaken en het bleek kinderlijk eenvoudig om van willekeurige mensen berichten, wachtwoorden, geslacht, seksuele voorkeur, afkomst, hobby's, koopgedrag en zelfs bankgegevens te achterhalen. Sindsdien log ik nooit meer onbeschermd in.

Lees hier het artikel

Hoe kun je wel veilig gebruik maken van een openbaar wifi-netwerk?

Er zijn maatregelen die je als treinreiziger of als terrasbezoeker kunt treffen. Dit zijn ze.

Lees het artikel hier

Wat metadata allemaal over je zeggen

Een lezer van De Correspondent toonde aan: die metadata verraden véél meer over je leven dan je denkt.

Lees het artikel

Enkele tips om jezelf digitaal te wapenen

Digitale zelfbescherming is geen quick fix. Er bestaat geen knopje om op te