

Den Haag verontrust over 'ongeautoriseerde toegang' door Huawei-medewerkers bij KPN

Bas Knoop Jeroen Piersma Stijn van Gils 19 apr

Politici zijn hevig geschrokken van de ongeautoriseerde toegang die de Chinese producent van netwerkkapparatuur Huawei heeft gehad tot het mobiele netwerk van KPN. Ondertussen ontbreekt het nog aan bewijs dat Huawei daadwerkelijk heeft gespioneerd, stellen verschillende deskundigen.



Premier Mark Rutte met Huawei-oprichter Zhengfei Ren tijdens een eerder bezoek aan het bedrijf tijdens een handelsmissie aan China. Foto: Jerry Lampen/ANP

In het kort

- Huawei zou ongeautoriseerd toegang hebben gehad tot het netwerk van KPN.
 - Politici zijn erg geschrokken en willen dinsdag opheldering bij het vragenuurtje.
 - Hard bewijs voor spionage is niet geleverd, stellen deskundigen.
-

Het politieke imago van Huawei is in Nederland op een nieuw dieptepunt beland. Al jaren zijn er speculaties dat de Chinese producent van onder meer zendmasten en netwerkapparatuur zou hebben gespioneerd, maar concreet bewijs ontbrak. Zaterdag onthulde de Volkskrant echter dat medewerkers van Huawei in 2010 daadwerkelijk 'ongeautoriseerde en ongecontroleerde toegang' zouden hebben gehad tot het mobiele netwerk van KPN.

Medewerkers van het Chinese bedrijf konden hierdoor onder andere gesprekken afluisteren, blijkt uit een rapport van consultancybedrijf Capgemini, waaruit de krant citeert. Via deze weg zou onder meer toenmalig premier Jan Peter Balkenende afgeluisterd kunnen zijn. Ook nu zouden medewerkers nog steeds ongecontroleerde toegang hebben, schrijft de krant maandag. Huawei zelf ontkent overigens.

Geen hard bewijs

Hard bewijs voor spionage is hiermee niet geleverd, zeggen verschillende deskundigen. De berichtgeving laat immers slechts zien dat Huawei toegang had tot gegevens en ook dat er ongeautoriseerd gebruik van zou zijn gemaakt, maar niet met welk doel, legt Sietse van der Gaast, consultant bij adviesbureau Stratix uit. Het zou dus spionage kunnen zijn, maar evengoed weliswaar ongeautoriseerde, maar verder goedbedoelde technische controles of reparaties. 'Er wordt met het oog van nu gekeken naar wat er toen mogelijk is gebeurd', zegt Mark Beermann, consultant bij Enterprise Summit.

En dat leden van het kabinet via het KPN-netwerk door Huawei werden afgeluisterd, vindt Hendrik Rood, consultant bij Stratix onwaarschijnlijk. Al ruim voor 2010 is de Rijksoverheid volgens hem overgeschakeld van KPN op Vodafone voor de mobiele dienstverlening. Vodafone werkt niet met Huawei-apparatuur. Het rapport van Capgemini heeft bovendien hoogstwaarschijnlijk slechts betrekking op KPN-dochter Telfort. 'Toen het rapport werd vervaardigd, werkte KPN zelf nog grotendeels met Ericsson-apparatuur.' Pas bij de introductie van 4G in 2012 was KPN volledig overgeschakeld.

'Bedreiging staatsveiligheid'

De onthullingen zijn niettemin hard geland in Den Haag. Verschillende partijen willen dinsdag van demissionair staatssecretaris Mona Keijzer (Economische Zaken en Klimaat, CDA) uitleg tijdens het wekelijkse vragenuur. 'Het was kennelijk jarenlang mogelijk voor Huawei om mobiele nummers van KPN af te luisteren', zegt Lisa van Ginneken, Tweede Kamerlid voor D66. 'Dat bedreigt onze staatsveiligheid en bedrijfsgeheimen.' Ze is verbaasd dat KPN het rapport van Capgemini al die tijd verborgen wilde houden. 'Kennelijk gaat bij KPN het bedrijfsbelang voor de nationale veiligheid.'

Keijzers ministerie wijst erop dat het kabinet al verschillende stappen heeft gezet om spionage en misbruik tegen te gaan. Zo moeten KPN, VodafoneZiggo en T-Mobile vóór oktober 2022 extra maatregelen nemen, zoals screening van medewerkers, die de veiligheid van de kritieke onderdelen van hun mobiele netwerken aanscherpen. Kritieke onderdelen van die telecomnetwerken mogen bovendien alleen afkomstig zijn van 'betrouwbare leveranciers', zei Keijzer destijds.

De extra maatregelen zijn een uitwerking van de algemene maatregel van bestuur voor de telecomsector uit november 2019. Hiermee kan het kabinet telecombedrijven ook dwingen om bepaalde leveranciers te weren. Het gaat daarbij om partijen die 'nauwe banden hebben of onder invloed staan van een staat, die de intentie heeft een communicatienetwerk in Nederland te misbruiken'.

Het Chinese Huawei wordt hierin niet bij naam genoemd. Maar dat gebeurt mogelijk wel in de geheime beschikking die KPN, VodafoneZiggo en T-Mobile 'op korte termijn' ontvangen van het ministerie van Economische Zaken en Klimaat. Daarin staat of en welke apparatuur zij moeten weren uit de kritieke onderdelen van hun 5G-netwerk.

'Weren Huawei geen oplossing'

Volgens Ronald Prins, cyberexpert van Hunt & Hackett, is het weren van Huawei nauwelijks een oplossing. 'Internationaal zie je dat allerlei hackersgroepen telecomproviders binnen weten te dringen. Daar is Huawei dus niet voor nodig.'

Liever zou hij zien dat Nederlandse inlichtingendiensten hun aftapbevoegdheden ook gaan gebruiken om te controleren of Nederlandse data weglekken naar bijvoorbeeld China. Ook zou hij willen dat telecombedrijven in het algemeen meer eigen kennis in huis halen om zelf hun netwerk in de gaten te houden. 'Banken zien hun IT-beveiliging als hun kerntaak, maar telecomproviders gaan daar juist van weg. Overal ter wereld zie je dat providers het beheer van hun netwerk uitbesteden.'



Bas Knoop



Jeroen Piersma



Stijn van Gils



Meest gelezen



'Gekkenhuis' in cryptoland zorgt voor forse stijging dogecoin