

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2380

Vragen van het lid **Jansen** (SP) aan de minister van Economische Zaken over *het bericht dat slimme meters eenvoudig te hacken zijn* (ingezonden 6 april 2010).

Antwoord van minister **Van der Hoeven** (Economische Zaken) (ontvangen 3 mei 2010).

Vraag 1

Heeft u kennisgenomen van het artikel ««Smart» utility meters have security holes and can be hacked, expert finds»?¹

Antwoord 1

Ja.

Vraag 2 en 3

Welke technische en procedurele voorzorgen zijn er getroffen om de kans op hacken van de op de Nederlandse markt toegelaten slimme meters te minimaliseren?

Is uitgesloten dat hackers via de slimme meter de stroomtoevoer naar een gebouw afsluiten, bijvoorbeeld als voorbereiding op een inbraak? Kunt u dit onderbouwen?

Antwoord 2 en 3

Het waarborgen van de privacy en het zo goed mogelijk beveiligen van de meter en het dataverkeer is een voorwaarde voor een geslaagde invoering van de slimme meter in Nederland. Het is van het grootste belang om de risico's op hacken te minimaliseren en eventuele gevolgen moeten zoveel mogelijk beperkt zijn. Hiertoe stel ik eisen in wet- en regelgeving en treffen de netwerkbedrijven zelf op grote schaal voorzorgsmaatregelen. Het op voorhand absoluut uitsluiten van hacken is helaas echter niet mogelijk. Voorafgaand aan de start van de uitrol van de slimme meter zal op grond van het wetsvoorstel marktmodel (31 374) een algemene maatregel van bestuur worden vastgesteld waarin nadere eisen worden gesteld aan de meetinrichting. In dit besluit zullen ook nadere eisen worden gesteld aan de beveiliging van de meter. Verder zal in een ministeriële regeling worden voorgeschreven

¹ Associated Press, 26 maart 2010: ««Smart» utility meters have security holes and can be hacked, expert finds»:
http://www.syracuse.com/news/index.ssf/2010/03/smart_utility_meters_have_secu.html

dat de voorwaarden ten aanzien van de wijze van gegevensverwerking (Informatiecode), die door de NMa op voorstel van de netbeheerders en leveranciers zal worden vastgesteld, ook zien op de beveiliging van de gegevensverwerking tussen de slimme meter bij de consument, de netbeheerder en de leverancier, alsmede op wijze waarop over de naleving daarvan in de jaarverslagen van netbeheerders en leveranciers wordt gerapporteerd. Deze voorwaarden ten aanzien van de wijze van gegevensuitwisseling zien daarmee ook op de verplichting voor netbeheerders en leveranciers om een rapportagevorm te ontwikkelen om kleinverbruikers, via de jaarverslagen, te informeren over de wijze waarop zij bij de uitwisseling van gegevens verantwoording afleggen over de naleving van de Wet bescherming persoonsgegevens. De NMa zal deze rapportagevorm vastleggen in de Informatiecode, die moet voldoen aan de nadere eisen die daaraan in de hiervoor genoemde ministeriële regeling worden gesteld. De NMa wordt belast met het toezicht op het publiceren van deze verklaring in of bij de jaarrekening. Het College Bescherming Persoonsgegevens ziet toe op de wijze waarop netbeheerders en leveranciers de Wet bescherming persoonsgegevens naleven.

De netbeheerders zijn verantwoordelijk voor de uitrol en het beheer van slimme meters, inclusief de beveiliging. In de afgelopen periode hebben de netbeheerders, verenigd in Netbeheer Nederland, gewerkt aan technische en procedurele voorzorgsmaatregelen. Netbeheer Nederland heeft hierbij samengewerkt met afnemerorganisaties, zoals de Consumentenbond en de Vereniging Eigen Huis, en diverse experts, waaronder TNO, PWC en de Radboud Universiteit. Ook mijn departement is bij dit proces betrokken geweest. De voornaamste technische en procedurele voorzorgsmaatregelen die door de netbeheerders getroffen worden, hebben betrekking op het:

- beperken van de toegang tot de meter door het aantal toegangspoorten te minimaliseren en door gebruik te maken van authenticatiemethoden;
- versleutelen van de gegevens van en naar de meter binnen de slimme meter infrastructuur en in de draadloze communicatie van en naar de slimme meters;
- gebruik van per meter unieke beveiligingssleutels, en de onmogelijkheid om vanaf een meter andere meters te benaderen;
- opsporen van pogingen om meters te hacken door op verschillende plaatsen in de infrastructuur detectiemaatregelen te treffen, zodat door de netbeheerder snel opgetreden kan worden.

Netbeheer Nederland zorgt voor de vertaling van deze eisen en maatregelen in landelijk beleid voor de netbeheerders. Netbeheer Nederland heeft mij geïnformeerd dat dit beleid medio dit jaar gereed zal zijn voor publicatie. Dan zal de precieze formulering van deze voorzorgsmaatregelen van de netbeheerders bekend zijn. De kernpunten van deze voorzorgsmaatregelen worden vastgelegd in de hiervoor genoemde regelgeving. Netbeheerders zijn met elkaar overeengekomen om beveiligingsincidenten met elkaar te delen en opgedane kennis te gebruiken om de beveiliging te verbeteren, opdat binnen de sector een eenduidig beveiligingsniveau wordt gerealiseerd. Ik constateer kortom dat de netbeheerders veel in het werk stellen om tot een adequate beveiliging te komen.

Vraag 4 en 5

Hoe is de rechtsbescherming van de klanten van energiebedrijven geregeld in geval van manipulatie van slimme meters door derden?

Is er binnen de huidige wettelijke kaders voor de klant enig risico dat hij opdraait voor (een deel van) de directe en indirecte schade die kan ontstaan ten gevolge van de manipulatie van slimme meters door derden? Zo ja, welk risico?

Antwoord 4 en 5

Wanneer een klant schade lijdt door een manipulatie die door de netbeheerder redelijkerwijs te voorkomen was, dan kan de klant de netbeheerder aansprakelijk stellen, net zoals dat nu het geval is. Dit houdt in dat een netbeheerder aansprakelijk is indien de netbeheerder toerekenbaar tekort is geschoten in de beveiliging van de meter en de klant dientengevolge schade lijdt. Daarnaast is het zo dat indien door manipulatie de meter veel meer verbruik aangeeft dan werkelijk is verbruikt, aan de klant dit niet gerealiseerde verbruik niet in rekening gebracht mag worden. De klant zal dan

alleen het verbruik dat hij naar schatting heeft gehad in rekening worden gebracht.

Daarnaast is het normale aansprakelijkheidsrecht van toepassing. De klant kan de hacker aansprakelijk stellen voor de schade die de klant lijdt. Wanneer een hacker bijvoorbeeld niet getraceerd kan worden of als deze niet voldoende draagkrachtig is en de netbeheerder niet aansprakelijk is, dan kunnen situaties ontstaan waarin de klant de schade niet (volledig) kan verhalen. Bij andere vormen van criminaliteit is dit niet anders.

Vraag 6

Acht u dit risico acceptabel in het licht van het voornemen van de regering om – vroeg of laat – de slimme meters verplicht uit te rollen, waardoor de afnemers van energie opgezadeld worden met risico's waar ze nooit om gevraagd hebben?

Antwoord 6

Slimme meters zijn van belang voor een betaalbare, betrouwbare en duurzame energievoorziening. Ik zie daarom uit naar een geslaagde invoering van de meter. Het waarborgen van de privacy en het zo goed mogelijk beveiligen van de meter en het dataverkeer is daarvoor een voorwaarde. Het wetsvoorstel marktmodel, de aangekondigde Algemene Maatregel van Bestuur en ministeriële regeling, en de maatregelen van de sector die hiervoor zijn beschreven, vormen hiervoor een goede basis. Overigens hebben kleinverbruikers de mogelijkheid om de slimme meter, die door de netbeheerder te beschikking wordt gesteld, te weigeren. Ook kunnen ze er voor kiezen om het op afstand uitlezen van meterstanden aan of uit te laten zetten als ze een slimme meter hebben.