Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

>Retouradres Postbus 20010, 2500 EA Den Haag

De Voorzitter van de Tweede Kamer der Staten Generaal
Postbus 20018
2500 EA Den Haag

Postbus 20010
2500 EA Den Haag
www.minbzk.nl

Contact
T 079 320 50 50
F 070 320 07 33

Ons kenmerk
831a6927-or1-2.0

Uw kenmerk

Bijlagen
0

Datum 11 oktober 2013
Betreft De recente digitale aanval op Belgacom

Naar aanleiding van de berichtgeving over mogelijke digitale spionage door de Amerikaanse *National Security Agency* (NSA) en het Britse *Government Communications Headquarters* (GCHQ) heeft de Kamer op 18 september jl. verzocht nader te worden geïnformeerd (kenmerk 2013Z17695). Hierbij informeer ik u mede namens de minister van Veiligheid en Justitie en de minister van Economische Zaken.

DigiNotar

Het Kamerlid Van Raak (SP) heeft tijdens de regeling van werkzaamheden van 18 september jl. onder meer gerefereerd aan de inbreuk bij DigiNotar in 2011. Volgens mediaberichten van 13 september jl. op onder meer de website www.schneier.com zou uit een afbeelding van een presentatie blijken dat de Amerikaanse NSA verantwoordelijk is voor, dan wel gebruik heeft gemaakt van deze inbreuk. Deze conclusie is volgens de Nederlandse regering onjuist. Er is geen aanleiding te veronderstellen dat de NSA verantwoordelijk is voor, of gebruik heeft gemaakt van de inbreuk bij DigiNotar.

Belgacom

Het Duitse tijdschrift Der Spiegel en de Belgische krant De Standaard hebben op 20 september jl. bericht over mogelijke digitale spionageactiviteiten van de NSA en van het GCHQ via een inbreuk op de infrastructuur van de Belgische aanbieder van telecommunicatie Belgacom. Op 3 oktober jl. heeft de NOS nader over de aanval bericht. Belgacom onderzoekt de herkomst van de aanval. De berichten bevestigen dat de veiligheid van onze digitale wereld de aandacht vraagt. De AIVD doet onderzoek naar aanleiding van de berichten. Er zijn vooralsnog geen aanwijzingen dat Nederland een direct doelwit is van de inbreuk.

De inbreuk bij KPN in het voorjaar van 2012 was overigens geen activiteit van een statelijke actor. KPN heeft naar aanleiding van die inbreuk aanvullende veiligheidsmaatregelen genomen.

Verantwoordelijkheden

Private partijen, waaronder aanbieders van openbare telecommunicatiediensten, zijn zelf verantwoordelijk voor de veiligheid van hun infrastructuur. De Telecommunicatiewet (Tw) bevat voor deze aanbieders verplichtingen voor de borging van de integriteit en de veiligheid van hun netwerken en diensten, waaronder het waarborgen van de vertrouwelijkheid van telecommunicatie en de beschikbaarheid van de dienstverlening. Het gaat daarbij om technische en organisatorische maatregelen. De grote aanbieders zetten hiervoor structureel eigen capaciteit in. Ook is inzet van expertise van derden mogelijk. De recente berichten in de media onderstrepen het belang van deze maatregelen. Indien daar

aanleiding voor is, kan de aanbieder worden verplicht bepaalde technische of organisatorische maatregelen te nemen of een veiligheidscontrole door een onafhankelijke deskundige te laten uitvoeren (art. 11a.1 vijfde resp. zesde lid van de Telecommunicatiewet).

Op basis van artikel 6 van de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 doet de AIVD onderzoek naar organisaties en personen die een gevaar vormen voor het voortbestaan van de democratische rechtsorde, de nationale veiligheid of andere gewichtige belangen van de staat. De AIVD is op basis van deze taak belast met het onderzoek naar contra-inlichtingen. Het onderzoek naar digitale spionage maakt daar deel van uit. De AIVD heeft onder meer een methodiek ontwikkeld voor de analyse van kwetsbaarheden voor spionage. Digitale spionage is daarbij één van de aandachtspunten. Deze methodiek is bij de vitale sectoren onder de aandacht gebracht.

Dreigingen en risico's

De AIVD en het Nationaal Cyber Security Centrum hebben herhaaldelijk gewezen op de kwetsbaarheden van de Nederlandse ICT-infrastructuur en de dreiging van digitale spionage. Het Cyber Security Beeld Nederland, dat onder coördinatie van het Nationaal Cyber Security Centrum met medewerking van de AIVD tot stand is gekomen, benoemt cybercrime en cyberspionage als de belangrijkste dreigingen. Onze afhankelijkheid van ICT is aanzienlijk, en de kwetsbaarheid van onze ICT is hoog. Digitale aanvallen worden daarnaast steeds complexer en geavanceerder. Dit najaar ontvangt u de nieuwe Nationale Cyber Security Strategie, waarin de regering onder meer meldt hoe deze dreigingen worden geadresseerd.

EU

Naar aanleiding van de onthullingen van de heer Snowden over onder meer het Amerikaanse programma PRISM is een gezamenlijke expertgroep van de EU en de VS opgericht. Deze expertgroep bespreekt de onthullingen in de media en de schendingen van de privacy van burgers. De Nederlandse regering steunt het werk van de expertgroep. Op 13 september jl. bent u over de voortgang geïnformeerd. Op 19 en 20 september jl. heeft een vervolgbijeenkomst van de expertgroep plaatsgevonden. De VS heeft in de bijeenkomsten onder meer gedetailleerde informatie verschaft over het toezicht op de inlichtingenvergaring. Naar verwachting volgen de volgende bijeenkomst en het eindrapport in het najaar.

Op 4 juli jl. heeft het Europees Parlement een resolutie aangenomen, waarin het zijn commissie voor burgerlijke vrijheden, justitie en binnenlandse zaken opdraagt de berichten grondig te onderzoeken. Daarbij worden onder meer de gevolgen van spionageprogramma's voor de grondrechten van EU-burgers en de mogelijkheden voor administratief en gerechtelijk verhaal bezien. In dat kader worden dit najaar in het Europees Parlement hoorzittingen gehouden. De hoorzittingen zijn inmiddels gestart. Een rapport van het onderzoek wordt voor het einde van het jaar verwacht.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk