> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
Der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directie Cyber Security

Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl

Kenmerk
5725010/12/NCTV

Datum 14 februari 2012
Betreft Hack bij KPN

Bij de regeling van werkzaamheden van donderdag 9 februari jl. heeft het lid Gesthuizen (SP) gevraagd om een brief over de hack bij KPN en in te gaan op de vraag hoe groot de dreiging voor het internetverkeer was en tot welke gegevens de hacker toegang had. Tevens wordt gevraagd in te gaan op het bericht dat de dreiging weg is, maar de hack nog niet is opgelost. Hierbij ontvangt u onze reactie op uw verzoek waarbij gebruik is gemaakt van de door KPN aan ons verstrekte informatie.

Alvorens in te gaan op dit incident merken wij op dat in deze, zich steeds verder digitaliserende maatschappij, het van cruciaal belang is dat elke organisatie uiterst zorgvuldig omgaat met klant- en of persoonsgegevens. Het betreft hier in veel gevallen een eigen verantwoordelijkheid van deze organisaties. Hierop is ook wet- en regelgeving van toepassing alsmede het toezicht daarop.

Inleiding
Op 18 januari heeft KPN een melding ontvangen van een mogelijke inbraak (hack) in haar serverclusters, die op 20 januari is geverifieerd. De eerste sporen van deze inbraak werden teruggetraceerd tot 16 januari. KPN heeft hierop op 20 januari direct beveiligingsmaatregelen genomen door de internet toegang waardoor de hacker is binnengedrongen af te sluiten. Tevens is een onderzoek gestart naar de oorzaak en de impact van de inbraak waarbij externe deskundigheid is ingeschakeld. Bij nader onderzoek bleek dat de hacker zich ook toegangsrechten op andere systemen heeft kunnen toe-eigenen. Hierop heeft KPN op 27 januari aan het Nationaal Cyber Security Centrum (NCSC) melding gemaakt van de hack en heeft zij het NCSC om assistentie gevraagd.

Nadat KPN melding heeft gemaakt van het incident is vanwege onduidelijkheid over de impact met de verschillende betrokken partijen zo goed als mogelijk een algemeen situatiebeeld gevormd. Daarnaast zijn andere relevante partijen door het NCSC geïnformeerd en zijn de acties op zowel beveiligingsgebied als op opsporingsgebied, op elkaar afgestemd.

Het NCSC monitorde de mogelijk bredere gevolgen dan alleen de technische kwestie bij KPN en heeft de coördinatie tussen de verschillende overheidspartijen op zich genomen. Hierbij lag de nadruk op de mogelijke gevolgen voor de (rijks)overheid, de nationale veiligheid en het internetverkeer. Zo is ondermeer

bezien welke onderdelen van de vitale infrastructuur zouden worden geraakt door de hack of de door KPN te nemen maatregelen, gevolgen voor 112 oproepen en eventuele congestie. Mede op basis van onderzoek van KPN (in samenwerking met ingehuurde veiligheidsexperts), het verkregen inzicht en de daaropvolgende maatregelen kon door de overheid worden geconcludeerd dat de nationale veiligheid niet in gevaar was.

Wegnemen dreiging
KPN heeft aangegeven dat zij maatregelen heeft genomen om eerst de dreiging weg te nemen en is er daarna toe overgegaan de hack structureel op te lossen. Zo is de hacker (of hackers) de toegang tot de systemen ontzegd en zijn extra beveiligingsmaatregelen genomen zoals het loskoppelen van servers van de operationele systemen van KPN. Hiermee was echter de hack, de door de hacker geëxploiteerde kwetsbaarheid in het systeem en eventueel door de hacker geïnstalleerde software, nog niet opgelost. In aanvulling op de eerdere maatregelen zijn na 27 januari de volgende acties uitgevoerd:

- herinstalleren en isoleren van systemen met klantinformatie;
- het installeren en veiligstellen van servers voor diensten zoals VOIP, zakelijke markt en iTV;

Bovenstaande acties zijn op 3 februari jl. afgerond. Daarnaast loopt nog het eigen forensisch onderzoek van KPN en worden alle overige servers preventief gescand. KPN geeft aan op dit moment alle denkbare en mogelijke veiligheidsmaatregelen te hebben getroffen waarbij een 100% garantie nooit te geven is.

Gecompromitteerde gegevens en dreiging voor het internetverkeer
Uit informatie van KPN blijkt dat de hacker (of hackers) toegang tot een aantal servers heeft verkregen en zich rechten heeft toegeëigend. Deze servers werden gebruikt voor websites, routering van internet gebaseerde diensten en opslag van (klant)informatie. Uit nog lopend onderzoek van KPN is niet gebleken dat de hacker klantinformatie heeft gekopieerd of anderszins heeft gemanipuleerd.
De hacker heeft ook rechten gehad op de DNS (Domain Name Server) systemen en heeft gebruikersrechten gehad op 1 van de routers. Daarmee had hij tijdelijk de routering van het internetverkeer van de consumentenklanten van KPN kunnen beïnvloeden. Aangezien via deze routering ook de Voice over IP dienstverlening loopt en daarmee bijvoorbeeld ook de 112 oproepen van klanten via VOIP (dus niet via de zogenaamde analoge aansluitingen of mobiele telefonie of mobiel internet) werd de dreiging serieus genomen en zijn passende maatregelen genomen. KPN meldt dat er geen bewijzen gevonden zijn dat oneigenlijke routering van internetverkeer heeft plaatsgevonden.

KPN heeft inmiddels aangekondigd versnelde investeringen door te voeren in haar IT- systemen om de veiligheid van die systemen te verhogen en er daarmee voor te zorgen dat de klanten van KPN zo veilig mogelijk van de diensten van KPN gebruik kunnen maken.

Actuele ontwikkelingen
Afgelopen vrijdag 10 februari jl. kwam het bericht naar buiten dat een hacker klantgegevens van KPN heeft gepubliceerd. Daarmee werd een relatie gelegd met de hierboven genoemde hack. KPN heeft toen uit voorzorg, in het kader van de bescherming van klantgegevens, de webmailfunctie voor circa 2 miljoen klanten tijdelijk afgesloten. Echter, uit nader onderzoek is gebleken dat de gepubliceerde gegevens niet van KPN afkomstig waren maar van een website waar klanten hun emailadres van KPN hebben achtergelaten.

Het is te betreuren dat hackers met manipulatie van een eerder gehackt databestand klanten onnodige last hebben bezorgd.

Stand van zaken relevante moties, toezeggingen en wetgevingstrajecten
Middels de kamerbrede motie Hennis-Plasschaert heeft uw Kamer de regering verzocht over te gaan tot een wettelijke meldplicht, een zogenaamde 'security breach notification'. Op 23 december heb ik uw Kamer geïnformeerd dat uw Kamer vóór het zomerreces van 2012 nader zal worden geïnformeerd over de wijze waarop deze meldplicht zal worden ingericht.[1]

Het wetsvoorstel tot wijzinging van de Telecomwet dat thans ter behandeling voorligt in de Eerste Kamer voorziet in twee meldplichten voor aanbieders van openbare elektronische communicatienetwerken en diensten waarbij het gaat om enerzijds inbreuken die een nadelig effect hebben op de bescherming van persoonsgegevens en anderzijds om inbreuken op de veiligheid waardoor de continuïteit in belangrijke mate wordt verbroken.

Daarnaast wil ik u erop wijzen dat Staatssecretaris Teeven een wetsvoorstel in consultatie heeft gezonden waarin een meldplicht voor datalekken is neergelegd. Wanneer dat wetsvoorstel te zijner tijd wordt aangenomen, is voorzien in een aanzienlijke verscherping van de regelgeving.

Uiteraard zal het incident eveneens worden bezien in het licht van de uitvoering van de motie Gesthuizen waarin de regering wordt verzocht om een visie op de privacy, veiligheid en bescherming van burgers op internet. Deze visie zal in het voorjaar aan uw Kamer worden aangeboden.[2]

Tot slot
KPN is een particulier bedrijf en is daarmee primair verantwoordelijk voor de beveiliging van haar systemen en de respons op dit incident. Tevens heeft KPN op basis van de Telecomwet een zorgplicht ten aanzien van haar klanten door passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van netwerken en diensten.

De toezichthouder Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA) heeft afgelopen zaterdag bekend gemaakt een onderzoek in te stellen of KPN op passende wijze invulling heeft gegeven aan deze zorgplicht.

De lopende onderzoeken van KPN en de OPTA zullen meer helderheid moeten verschaffen over wat precies is voorgevallen, het moment van melden van het incident, in hoeverre de aanpak juist geweest is en hoe in de toekomst deze situaties te voorkomen zijn, dan wel van een adequate response met bijbehorende communicatie voorzien kunnen worden.

[1] *Zie Kamerstukken 2010/11, 26 643 nr. 202*
[2] *Zie Kamerstukken II 2011/12 24 095 nr.294*

Daarnaast wordt onder de verantwoordelijkheid van het OM in samenwerking met het High Tech Crime Unit van de Nationale Recherche momenteel een strafrechtelijk onderzoek uitgevoerd naar de digitale inbraak bij KPN.

Datum
14 februari 2012

Kenmerk
5725010/12/NCTV

De Minister van Veiligheid en Justitie,

I.W. Opstelten

De Minister van Economische Zaken, Landbouw en Innovatie,

drs. M.J.M. Verhagen