Wob-verzoek Vodafone Voicemail

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Map 4

Stuk nummer 294 t/m 391

294

[redacted]

Van: [redacted]
Verzonden: woensdag 30 maart 2011 15:34
Aan: [redacted]
CC: [redacted]
Onderwerp: Stand van zaken voicemail incident

Geachte heer [redacted]

In de bijlage treft u een brief aan uit naam van de heer [redacted] alsmede de heer [redacted] inzake de stand van zaken omtrent het voicemail incident.

Met vriendelijke groet,

[redacted]

A to [redacted]

Tel: [redacted]
E-mail [redacted]
Web: www.vodafone.nl

Vodafone Netherlands
KvK-nummer 14052264
Kingsfordweg 43, 1043 GP Amsterdam
Postbus 59095, 1040 KB Amsterdam

[redacted]
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. de [redacted]
[redacted]
Schedeldoekshaven 200
2511 EA DEN HAAG

[redacted]
[redacted]
Onderwerp: voicemail incidenten

30 maart 2011

Geachte [redacted]

Naar aanleiding van de voicemail incidenten van vorige week en refererend aan de eerdere contacten die wij hieromtrent met u hebben gehad, geven wij hieronder een overzicht van de stand van zaken. .

Vodafone biedt, net als de nadere operators, de mogelijkheid aan om voicemail vanaf je eigen mobiel of vanaf een ander vast of mobiel nummer te benaderen. Voor het uitluisteren van voicemail van afstand (vanaf een vaste lijn of vanuit een ander mobiel netwerk) is voor alle zakelijke klanten normaal gesproken vereist dat de gebruiker zelf een eigen pincode instelt. Bij een upgrade van ons voicemail systeem op 16 november van het afgelopen jaar is dit onderdeel in de herconfiguratie per abuis achterwege gelaten. Hierdoor werd het voor gebruikers mogelijk om van afstand, zonder verdere actie, via de standaardcode "3333" toegang te krijgen tot hun voicemail.

Vorige week woensdag 23 maart jl. werden we door Een Vandaag geconfronteerd met de mogelijkheid van misbruik door onbevoegde derden in bezit van het mobiele nummer van de gebruiker. Onbevoegde derden hebben de mogelijkheid gehad om berichten te beluisteren die in de voicemails van bewindslieden en topambtenaren zijn achtergelaten, waaronder eventueel berichten met een privékarakter of van vertrouwelijke aard.. Wij hebben daarop de voicemail teruggezet naar de originele configuratie, nu ook voor consumenten. Dit is geïmplementeerd nog voordat deze mogelijkheid door de uitzending van Een Vandaag bij het grote publiek bekend werd.

Vervolgens hebben wij onze aandacht gericht op de situatie waarbij een beller vanaf een ander netwerk dan het Vodafone netwerk zich voordoet als Vodafone klant, het zogenaamde spoofing. Bij deze vorm van internetmisdaad kunnen onbevoegden beveiligingsmaatregelen omzeilen en toegang krijgen tot de voicemail, zonder dat daarbij naar de pincode wordt gevraagd. Spoofing is op zich niet nieuw in de digitale wereld. In januari van dit jaar hebben wij GovCert geïnformeerd dat gebruikers zich kunnen beveiligen tegen ID spoofing door via het IVR-menu een extra beveiliging te activeren. Deze extra beveiliging komt er op neer dat de eindgebruiker zelf instelt dat hij of zij altijd om een pincode moet vragen om de voicemail uit te luisteren, dus ook als je met je eigen toestel in Nederland belt. Wij hebben begrepen dat GovCert haar eindgebruikers vervolgens heeft gewaarschuwd voor spoofing en hen heeft aanbevolen de hiervoor omschreven extra beveiliging per direct te activeren. Iedereen die deze aanbeveling heeft opgevolgd, was al beveiligd tegen voicemail spoofing.

Vodafone
Kingsfordweg 43
1043 GP Amsterdam
Telefoon +31 (0)43 – 3555 555
vodafone.nl

Tevens hebben wij aangekondigd dat wij op een zo kort mogelijke termijn structurele maatregelen tegen spoofing zouden invoeren waarbij zoveel mogelijk rekening zou worden gehouden met het gebruikersgemak. Door de berichtgeving sinds woensdag over de kwetsbaarheid van voicemail is het risico op misbruik zodanig toegenomen dat versnelde invoering van maatregelen helaas nodig was. Daar is sinds woensdagavond 23 maart jl. aan gewerkt en die nacht zijn deze maatregelen succesvol geïmplementeerd. Hierdoor is het nu ook voor iedereen die vanaf een ander netwerk dan het Vodafone netwerk in Nederland naar zijn voicemail belt, verplicht een persoonlijke pincode in te voeren. Onbevoegde toegang tot voicemail is nu niet meer mogelijk. Vrijdagochtend heeft Govcert testen uitgevoerd en ons bevestigd dat de beveiliging tegen voicemail spoofing adequaat werkt.

In aanvulling op het voorstaande hebben wij wij in samenwerking met onafhankelijke experts en onze vaste partners een versnelde audit uitgevoerd om ons netwerk en onze systemen te toetsen aan onze aangescherpte veiligheidsnormen. De resultaten daarvan hebben wij de afgelopen dagen met u gedeeld.

Als volgende stap is nu een security task force ingesteld met als doel het herdefiniëren van de veiligheidsstandaarden in onze systemen en processen in het licht van de nieuwe eisen. Daarbij zullen wij in ieder geval ook Govcert betrekken.

Vanzelfsprekend begrijpen wij de noodzaak van een onderzoek naar de omvang van het mogelijke misbruik dat er in de afgelopen periode van voicemail van bewindslieden is gemaakt. Wij zijn uiteraard bereid hieraan mee te werken en zijn thans met u in overleg hoe wij binnen de grenzen van de relevante privacywet- en regelgeving zo snel en efficiënt mogelijk de omvang en aard van het mogelijke misbruik kunnen vaststellen.

Wij gaan ervan uit u hiermee vooralsnog voldoende te hebben geïnformeerd. Wij betreuren het incident en bieden onze excuses aan voor het ontstane ongemak. Het mag duidelijk zijn dat wij alles op alles zetten om in samenwerking met u te zorgen dat dit een eenmalige situatie was. Hiertoe zullen wij een structureel overleg opzetten. Wij menen dat wij hierdoor ook op een goede manier invulling kunnen geven aan het strategisch contractmanagement en beter in staat zullen zijn om de onderlinge verwachtingen op elkaar af te stemmen.

Mocht u naar aanleiding van het bovenstaande nog vragen hebben, dan kunt u uiteraard te allen tijde contact met mij opnemen.

Met vriendelijke groet,

[redacted]

295

[redacted]

Van: [redacted]
Verzonden: woensdag 30 maart 2011 18:15
Aan: [redacted]
Onderwerp: FW: Stand van zaken voicemail incident

Ha[redacted]
Is dit zoals afgesproken? Gaan wij hier nog op reageren en op welke wijze: brief of mail?
Groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 30 maart 2011 15:34
Aan: [redacted]
CC: [redacted]
Onderwerp: Stand van zaken voicemail incident

Geachte heer[redacted]

In de bijlage treft u een brief aan uit naam van de heer[redacted], alsmede de heer[redacted], inzake de stand van zaken omtrent het voicemail incident.

Met vriendelijke groet,

[redacted]

[redacted]

Tel: [redacted]
E-mail: [redacted]
Web: www.vodafone.nl

Vodafone Netherlands
KvK-nummer 14052264
[redacted]ngsfordweg 43, 1043 GP Amsterdam
[redacted]ostbus 59095, 1040 KB Amsterdam
(Disclaimer)
This message and any files or documents attached are strictly confidential or otherwise legally protected. It is intended only for the individual or entity named. If you are not the named addressee or have received this email in error, please inform the sender immediately, delete it from your system and do not copy or disclose it or its contents or use it for any purpose. Please also note that transmission cannot be guaranteed to be secure or error-free.

[redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. de [redacted]
Schedeldoekshaven 200
2511 EA DEN HAAG

[redacted]

Onderwerp: voicemail incidenten

30 maart 2011

Geachte [redacted]

Naar aanleiding van de voicemail incidenten van vorige week en refererend aan de eerdere contacten die wij hieromtrent met u hebben gehad, geven wij hieronder een overzicht van de stand van zaken..

Vodafone biedt, net als de nadere operators, de mogelijkheid aan om voicemail vanaf je eigen mobiel of vanaf een ander vast of mobiel nummer te benaderen. Voor het uitluisteren van voicemail van afstand (vanaf een vaste lijn of vanuit een ander mobiel netwerk) is voor alle zakelijke klanten normaal gesproken vereist dat de gebruiker zelf een eigen pincode instelt. Bij een upgrade van ons voicemail systeem op 16 november van het afgelopen jaar is dit onderdeel in de herconfiguratie per abuis achterwege gelaten. Hierdoor werd het voor gebruikers mogelijk om van afstand, zonder verdere actie, via de standaardcode "3333" toegang te krijgen tot hun voicemail.

Vorige week woensdag 23 maart jl. werden we door Een Vandaag geconfronteerd met de mogelijkheid van misbruik door onbevoegde derden in bezit van het mobiele nummer van de gebruiker. Onbevoegde derden hebben de mogelijkheid gehad om berichten te beluisteren die in de voicemails van bewindslieden en topambtenaren zijn achtergelaten, waaronder eventueel berichten met een privékarakter of van vertrouwelijke aard.. Wij hebben daarop de voicemail teruggezet naar de originele configuratie, nu ook voor consumenten. Dit is geïmplementeerd nog voordat deze mogelijkheid door de uitzending van Een Vandaag bij het grote publiek bekend werd.

Vervolgens hebben wij onze aandacht gericht op de situatie waarbij een beller vanaf een ander netwerk dan het Vodafone netwerk zich voordoet als Vodafone klant, het zogenaamde spoofing. Bij deze vorm van internetmisdaad kunnen onbevoegden beveiligingsmaatregelen omzeilen en toegang krijgen tot de voicemail, zonder dat daarbij naar de pincode wordt gevraagd. Spoofing is op zich niet nieuw in de digitale wereld. In januari van dit jaar hebben wij GovCert geïnformeerd dat gebruikers zich kunnen beveiligen tegen ID spoofing door via het IVR-menu een extra beveiliging te activeren. Deze extra beveiliging komt er op neer dat de eindgebruiker zelf instelt dat hij of zij altijd om een pincode moet vragen om de voicemail uit te luisteren, dus ook als je met je eigen toestel in Nederland belt. Wij hebben begrepen dat GovCert haar eindgebruikers vervolgens heeft gewaarschuwd voor spoofing en hen heeft aanbevolen de hiervoor omschreven extra beveiliging per direct te activeren. Iedereen die deze aanbeveling heeft opgevolgd, was al beveiligd tegen voicemail spoofing.

Tevens hebben wij aangekondigd dat wij op een zo kort mogelijke termijn structurele maatregelen tegen spoofing zouden invoeren waarbij zoveel mogelijk rekening zou worden gehouden met het gebruikersgemak. Door de berichtgeving sinds woensdag over de kwetsbaarheid van voicemail is het risico op misbruik zodanig toegenomen dat versnelde invoering van maatregelen helaas nodig was. Daar is sinds woensdagavond 23 maart jl. aan gewerkt en die nacht zijn deze maatregelen succesvol geïmplementeerd. Hierdoor is het nu ook voor iedereen die vanaf een ander netwerk dan het Vodafone netwerk in Nederland naar zijn voicemail belt, verplicht een persoonlijke pincode in te voeren. Onbevoegde toegang tot voicemail is nu niet meer mogelijk. Vrijdagochtend heeft Govcert testen uitgevoerd en ons bevestigd dat de beveiliging tegen voicemail spoofing adequaat werkt.

In aanvulling op het voorstaande hebben wij wij in samenwerking met onafhankelijke experts en onze vaste partners een versnelde audit uitgevoerd om ons netwerk en onze systemen te toetsen aan onze aangescherpte veiligheidsnormen. De resultaten daarvan hebben wij de afgelopen dagen met u gedeeld.

Als volgende stap is nu een security task force ingesteld met als doel het herdefiniëren van de veiligheidsstandaarden in onze systemen en processen in het licht van de nieuwe eisen. Daarbij zullen wij in ieder geval ook Govcert betrekken.

Vanzelfsprekend begrijpen wij de noodzaak van een onderzoek naar de omvang van het mogelijke misbruik dat er in de afgelopen periode van voicemail van bewindslieden is gemaakt. Wij zijn uiteraard bereid hieraan mee te werken en zijn thans met u in overleg hoe wij binnen de grenzen van de relevante privacywet- en regelgeving zo snel en efficiënt mogelijk de omvang en aard van het mogelijke misbruik kunnen vaststellen.

Wij gaan ervan uit u hiermee vooralsnog voldoende te hebben geïnformeerd. Wij betreuren het incident en bieden onze excuses aan voor het ontstane ongemak. Het mag duidelijk zijn dat wij alles op alles zetten om in samenwerking met u te zorgen dat dit een eenmalige situatie was. Hiertoe zullen wij een structureel overleg opzetten. Wij menen dat wij hierdoor ook op een goede manier invulling kunnen geven aan het strategisch contractmanagement en beter in staat zullen zijn om de onderlinge verwachtingen op elkaar af te stemmen.

Mocht u naar aanleiding van het bovenstaande nog vragen hebben, dan kunt u uiteraard te allen tijde contact met mij opnemen.

Met vriendelijke groet,

[redacted]

298

[redacted]

Van: [redacted]
Verzonden: donderdag 31 maart 2011 8:00
Aan: [redacted]
Onderwerp: RE: Stand van zaken voicemail incident

[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 30 maart 2011 18:20
Aan: [redacted]
Onderwerp: RE: Stand van zaken voicemail incident

[redacted]

[redacted]t,

Sent with Good (www.good.com)

-----Original Message-----
From: [redacted]
Sent: Wednesday, March 30, 2011 06:14 PM W. Europe Standard Time
To: [redacted]
Subject: FW: Stand van zaken voicemail incident

Ha [redacted]
Is dit zoals afgesproken? Gaan wij hier nog op reageren en op welke wijze: brief of mail? Groet[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 30 maart 2011 15:34
Aan: [redacted]
Onderwerp: Stand van zaken voicemail incident

Geachte heer[redacted]

In de bijlage treft u een brief aan uit naam van de heer [redacted]
alsmede de heer [redacted]nzake de stand van zaken omtrent het voicemail incident.

Met vriendelijke groet,

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl <http://www.vodafone.nl/>

Vodafone Netherlands

KvK-nummer 14052264

Kingsfordweg 43, 1043 GP Amsterdam

Postbus 59095, 1040 KB Amsterdam

300

[redacted]

Van: [redacted]
Verzonden: donderdag 31 maart 2011 15:14
Aan: [redacted]
Onderwerp: FW: Stand van zaken voicemail incident

tkn
-----Oorspronkelijk bericht-----
Van: S[redacted]
Verzonden: woensdag 30 maart 2011 15:34
Aan: [redacted]
CC: [redacted]
Onderwerp: Stand van zaken voicemail incident

Geachte heer [redacted]

In de bijlage treft u een brief aan uit naam van de heer [redacted], [redacted] alsmede de heer [redacted], inzake de stand van zaken omtrent het voicemail incident.

Met vriendelijke groet,

[redacted]

[redacted]

Tel: [redacted]
E-mail: [redacted]
Web: www.vodafone.nl

[redacted]
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. de[redacted]
Directeur-Generaal Organisatie en Bedrijfsvoering Rijk
Schedeldoekshaven 200
2511 EA DEN HAAG

[redacted]
E[redacted]
Onderwerp: voicemail incidenten

30 maart 2011

Geachte[redacted]

Naar aanleiding van de voicemail incidenten van vorige week en refererend aan de eerdere contacten die wij hieromtrent met u hebben gehad, geven wij hieronder een overzicht van de stand van zaken. .

Vodafone biedt, net als de nadere operators, de mogelijkheid aan om voicemail vanaf je eigen mobiel of vanaf een ander vast of mobiel nummer te benaderen. Voor het uitluisteren van voicemail van afstand (vanaf een vaste lijn of vanuit een ander mobiel netwerk) is voor alle zakelijke klanten normaal gesproken vereist dat de gebruiker zelf een eigen pincode instelt. Bij een upgrade van ons voicemail systeem op 16 november van het afgelopen jaar is dit onderdeel in de herconfiguratie per abuis achterwege gelaten. Hierdoor werd het voor gebruikers mogelijk om van afstand, zonder verdere actie, via de standaardcode "3333" toegang te krijgen tot hun voicemail.

Vorige week woensdag 23 maart jl. werden we door Een Vandaag geconfronteerd met de mogelijkheid van misbruik door onbevoegde derden in bezit van het mobiele nummer van de gebruiker. Onbevoegde derden hebben de mogelijkheid gehad om berichten te beluisteren die in de voicemails van bewindslieden en topambtenaren zijn achtergelaten, waaronder eventueel berichten met een privékarakter of van vertrouwelijke aard.. Wij hebben daarop de voicemail teruggezet naar de originele configuratie, nu ook voor consumenten. Dit is geïmplementeerd nog voordat deze mogelijkheid door de uitzending van Een Vandaag bij het grote publiek bekend werd.

Vervolgens hebben wij onze aandacht gericht op de situatie waarbij een beller vanaf een ander netwerk dan het Vodafone netwerk zich voordoet als Vodafone klant, het zogenaamde spoofing. Bij deze vorm van internetmisdaad kunnen onbevoegden beveiligingsmaatregelen omzeilen en toegang krijgen tot de voicemail, zonder dat daarbij naar de pincode wordt gevraagd. Spoofing is op zich niet nieuw in de digitale wereld. In januari van dit jaar hebben wij GovCert geïnformeerd dat gebruikers zich kunnen beveiligen tegen ID spoofing door via het IVR-menu een extra beveiliging te activeren. Deze extra beveiliging komt er op neer dat de eindgebruiker zelf instelt dat hij of zij altijd om een pincode moet vragen om de voicemail uit te luisteren, dus ook als je met je eigen toestel in Nederland belt. Wij hebben begrepen dat GovCert haar eindgebruikers vervolgens heeft gewaarschuwd voor spoofing en hen heeft aanbevolen de hiervoor omschreven extra beveiliging per direct te activeren. Iedereen die deze aanbeveling heeft opgevolgd, was al beveiligd tegen voicemail spoofing.

Tevens hebben wij aangekondigd dat wij op een zo kort mogelijke termijn structurele maatregelen tegen spoofing zouden invoeren waarbij zoveel mogelijk rekening zou worden gehouden met het gebruikersgemak. Door de berichtgeving sinds woensdag over de kwetsbaarheid van voicemail is het risico op misbruik zodanig toegenomen dat versnelde invoering van maatregelen helaas nodig was. Daar is sinds woensdagavond 23 maart jl. aan gewerkt en die nacht zijn deze maatregelen succesvol geïmplementeerd. Hierdoor is het nu ook voor iedereen die vanaf een ander netwerk dan het Vodafone netwerk in Nederland naar zijn voicemail belt, verplicht een persoonlijke pincode in te voeren. Onbevoegde toegang tot voicemail is nu niet meer mogelijk. Vrijdagochtend heeft Govcert testen uitgevoerd en ons bevestigd dat de beveiliging tegen voicemail spoofing adequaat werkt.

In aanvulling op het voorstaande hebben wij wij in samenwerking met onafhankelijke experts en onze vaste partners een versnelde audit uitgevoerd om ons netwerk en onze systemen te toetsen aan onze aangescherpte veiligheidsnormen. De resultaten daarvan hebben wij de afgelopen dagen met u gedeeld.

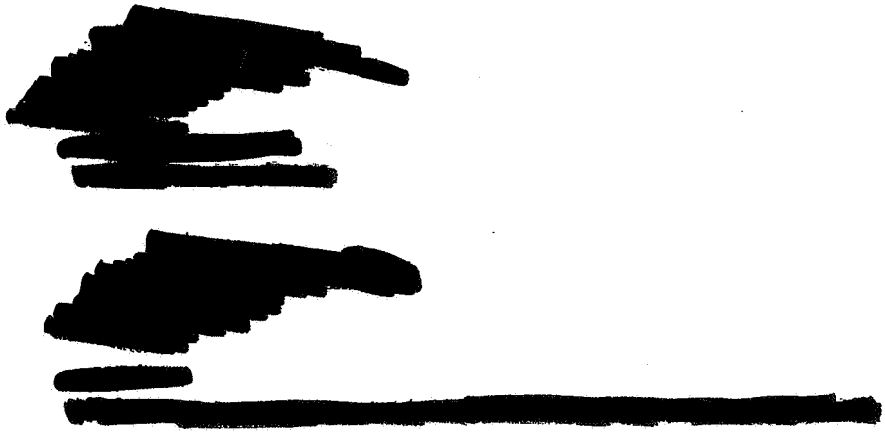
Als volgende stap is nu een security task force ingesteld met als doel het herdefiniëren van de veiligheidsstandaarden in onze systemen en processen in het licht van de nieuwe eisen. Daarbij zullen wij in ieder geval ook Govcert betrekken.

Vanzelfsprekend begrijpen wij de noodzaak van een onderzoek naar de omvang van het mogelijke misbruik dat er in de afgelopen periode van voicemail van bewindslieden is gemaakt. Wij zijn uiteraard bereid hieraan mee te werken en zijn thans met u in overleg hoe wij binnen de grenzen van de relevante privacywet- en regelgeving zo snel en efficiënt mogelijk de omvang en aard van het mogelijke misbruik kunnen vaststellen.

Wij gaan ervan uit u hiermee vooralsnog voldoende te hebben geïnformeerd. Wij betreuren het incident en bieden onze excuses aan voor het ontstane ongemak. Het mag duidelijk zijn dat wij alles op alles zetten om in samenwerking met u te zorgen dat dit een eenmalige situatie was. Hiertoe zullen wij een structureel overleg opzetten. Wij menen dat wij hierdoor ook op een goede manier invulling kunnen geven aan het strategisch contractmanagement en beter in staat zullen zijn om de onderlinge verwachtingen op elkaar af te stemmen.

Mocht u naar aanleiding van het bovenstaande nog vragen hebben, dan kunt u uiteraard te allen tijde contact met mij opnemen.

Met vriendelijke groet,



303

[redacted]

Van: [redacted]
Verzonden: donderdag 31 maart 2011 16:16
Aan: [redacted]
Onderwerp: RE: Jij belde?

[redacted]

Sent with Good (www.good.com)

-----Original Message-----
From: [redacted]
Sent: Thursday, March 31, 2011 04:12 PM W. Europe Standard Time
To: [redacted]
Subject: RE: Jij belde?

[redacted] heeft morgen een belafspraak met heer [redacted] over brief van Vodafone (zij [redacted] en dit gevraagd). Moet hij daar nog iets voor weten? Groet [redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 31 maart 2011 16:11
Aan: [redacted]
Onderwerp: Jij belde?

Ik zit bij een bijeenkomst. Moet ik nog bellen?

Sent with Good (www.good.com)

304

[redacted]

Van: [redacted]
Verzonden: donderdag 31 maart 2011 16:18
Aan: [redacted]
Onderwerp: RE: Jij belde?

[redacted]
groet

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 31 maart 2011 16:16
Aan: [redacted]
Onderwerp: RE: Jij belde?

[redacted]

with Good (www.good.com)

-----Original Message-----
From: [redacted]
Sent: Thursday, March 31, 2011 04:12 PM W. Europe Standard Time
To: [redacted]
Subject: RE: Jij belde?

[redacted] heeft morgen een belafspraak met heer [redacted] over brief van Vodafone (zij hebben dit gevraagd). Moet hij daar nog iets voor weten? Groet [redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 31 maart 2011 16:11
Aan: [redacted]
Onderwerp: Jij belde?

Ik zit bij een bijeenkomst. Moet ik nog bellen?

Sent with Good (www.good.com)

307

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 10:06
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Stand van zaken voicemail incident

[redacted]
Zie: http://webwereld.nl/nieuws/106200/vodafone-beveiligt-voicemail-tegen-bruteforce.html

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....

inisterie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag |[redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 31 maart 2011 15:14
Aan: [redacted]
Onderwerp: FW: Stand van zaken voicemail incident

tkn
-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 30 maart 2011 15:34
Aan: [redacted]
CC: [redacted]
Onderwerp: Stand van zaken voicemail incident

Geachte heer [redacted]

In de bijlage treft u een brief aan uit naam van de heer [redacted], alsmede de heer [redacted] inzake de stand van zaken omtrent het voicemail incident.

Met vriendelijke groet,

[redacted]

[redacted]

Tel: [redacted]
E-mail: [redacted]

Web: www.vodafone.nl

Vodafone Netherlands
KvK-nummer 14052264
Kingsfordweg 43, 1043 GP Amsterdam
Postbus 59095, 1040 KB Amsterdam

Vodafone beveiligt voicemail tegen bruteforce

Gepubliceerd: Donderdag 31 maart 2011
Auteur: [redacted]

Vodafone treft ook maatregelen tegen het bruteforcen van de voicemailcode van ministers en andere abonnees. Dat was tot enkele dagen geleden namelijk wel mogelijk.

Telecomoperator Vodafone heeft een derde sluipweg om de voicemail van abonnees af te luisteren de pas afgesneden. Vorige week moest het bedrijf al vol aan de bak nadat bleek dat voicemailboxen wagenwijd openstonden door gebruik van standaard pincode 3333 of via CallerID spoofing.

Bruteforce aanval

Er is ook nog een derde methode: bruteforce, door achter elkaar verschillende codes uit te proberen totdat de juiste code wordt achterhaald. Zo achterhaalde Revu in december 2008 ook het wachtwoord van de privéwebmail van staatssecretaris [redacted].

Het achterhalen van de voicemailpin via bruteforce is relatief bewerkelijk omdat de verbinding na 3 foute codes wordt verbroken. Maar een nieuw belletje gaf wel weer steeds drie nieuwe pogingen. Met een pincode van 4 cijfers zijn er maximaal 10.000 combinaties mogelijk.

Behoorlijk omslachtig, maar wel te doen. En voor een belangrijk persoon als een topmanager of minister absoluut de moeite waard. Dat stelt een expert op het gebied van telecom, security en privacy tegenover Webwereld. Hij wil anoniem blijven.

Low tech

"Stel je bent een Chinees die geïnteresseerd is in wat [redacted] of een andere minister aan berichten binnenkrijgt, terwijl er een duikboot aan Taiwan verkocht gaat worden. Je schakelt even (heel goedkoop) 10 landgenoten in en die laat je elk maximaal 1000 keer bellen. Heel low tech, gewoon vanuit China (al dan niet met spoofing) en binnen hooguit 8 uur heb je de pin. Zonder veel kans op ontdekking."

Volgens [redacted], is deze methode inderdaad goed te doen. "Gemiddeld heb je 5000 pogingen nodig. Dus binnen een paar uur bellen kom je er wel achter. En grote kans dat mensen een voorspelbare code hebben, dus die moet je eerst proberen." Dat bleek ook vorige week, toen EenVandaag na paar keer proberen de voicemailcode van Rosenthal te pakken had.

Toch denkt Prins dat professionele cyberspionnen deze methode mijden, omdat het toch erg kan opvallen. "Dit is meer iets voor de media of een hackertje. Geheime diensten zullen eerder proberen het netwerk van de telco zelf te penetreren. Dan heb je ook meer keuze wie je af wilt luisteren."

Pinblokkade

Bruteforcen van Vodafone voicemails kon tot enkele dagen geleden dus wel, maar nu niet meer, benadrukt de operator. Na 6 foute codes is de voicemailbox een paar uur lang niet meer bereikbaar

vanaf een ander netwerk. De eigenaar kan dan trouwens nog wel met zijn eigen telefoon voicemail afluisteren via 1233.

Ook heeft het concern een maximum gesteld aan het aantal foute pincodes dat door een klant kan worden ingevoerd. Hoeveel precies wil het bedrijf niet kwijt. De kans dat de juiste code wordt geraden is hiermee gedecimeerd.

T-Mobile laat desgevraagd weten dat het vaak invoeren van foute voicemailpincodes "bij ons in het systeem wordt gezien." Daarnaast kunnen T-Mobile klanten ook een langere code aanmaken, tot 6 cijfers. "En met 6 cijfers heb je dus al een miljoen combinaties." KPN kon nog niet zeggen of ze maatregelen hebben genomen tegen de bruteforce methode.

Onderzoek naar staatsveiligheid

Minister Donner heeft eind vorige week in een reactie (pdf) een onderzoek aangekondigd naar mogelijk misbruik van de gaten in het voicemailsysteem van Vodafone en in hoeverre hierdoor "de staatsveiligheid in het geding is geweest." Er komt ook nog een spoeddebat in de Tweede Kamer over de kwestie.

Relevante whitepapers

- Grensoverschrijdende data
- Snelle, maar veilige applicatietoegang

308

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:42
Aan: [redacted]
Onderwerp: FW: maatregelen veilig bellen

Bij jou bekend?

Met vriendelijke groet,

mr drs [redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
Directie Informatiseringsbeleid Rijk
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:32
Aan: [redacted]
CC: [redacted]
Onderwerp: maatregelen veilig bellen

Hoi [redacted]

Ik hoorde dat de Kamercommissie BZK heeft gevraagd om op het punt 'op afstand aflusiten van mobiele telefoons bij de overheid' bewindspersonen worden verzocht de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven. De minister heeft de TK-leden verzocht uiterlijk do. 31 maart 16 u aanvullende onderwerpen aan te leveren over beveiliging communicatiemiddelen.

Denk dat jij de lead daarin hebt? Ik ben er graag bij betrokken.

Met vriendelijke groeten,

[redacted]

309

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:48
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: maatregelen veilig bellen

Gaat dit niet over Vodafone voicemail?

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag [redacted]
Postbus 20011 | 2500 EA | Den Haag
T [redacted]
[redacted]
http://www.minbzk.nl

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:32
Aan: [redacted]
CC: [redacted]
Onderwerp: maatregelen veilig bellen

Hoi [redacted]

Ik hoorde dat de Kamercommissie BZK heeft gevraagd om op het punt 'op afstand aflusiten van mobiele telefoons bij de overheid' bewindspersonen worden verzocht de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven. De minister heeft de TK-leden verzocht uiterlijk do. 31 maart 16 u aanvullende onderwerpen aan te leveren over beveiliging communicatiemiddelen.

Denk dat jij de lead daarin hebt? Ik ben er graag bij betrokken.

Met vriendelijke groeten,

[redacted]

310

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 12:23
Aan: [redacted]
Onderwerp: SMS spoofing media coverage

Ha [redacted]ik heb je net een voicemail ingesproken nav een item van Powned dat gisteravond op TV was en dat vanavond een vervolg uitzendt. Het gaat hier om een bekend industrie issue en dit is fundamenteel anders dan waar we verleden week mee te maken hadden. We hebben contact gehad met KPN en die hebben dit bevestigd. Zie ook een site als spoever.nl.

[redacted]

[redacted]

Hieronder nog het statement dat wij reactief zullen gebruiken.

Groet
[redacted]

Gisteravond liet Pownews zien dat het mogelijk is om via internet sms-berichten te versturen namens een andere, valse afzender. Dit betreft geen kwetsbaarheid in het mobiele netwerk, ook wordt er niet ingebroken in 'sms-boxen' van gebruikers. Pownews maakte gebruik van een premium (betaalde) sms spoofing dienst die op internet wordt aangeboden. De afzender en ontvanger van de sms kan daarbij zelf ingevuld worden. Met deze dienst wordt de identiteit van iemand anders nagebootst, wat illegaal is. Gebruikers van deze dienst hebben geen toegang tot de sms-berichten van de ogenschijnlijke zender of ontvanger.

Sms spoofing is een internationaal probleem en heeft in Nederland de aandacht van de industrie en overheid/Opta. De aanbieders van sms spoofing diensten versturen sms-berichten vanaf het internet via verschillende mobiele netwerken naar mobiele telefoons. Vodafone Nederland weert aanbieders van dergelijke sms spoofing diensten van zijn netwerk. Echter, dat neemt niet weg dat het mogelijk blijft om via andere netwerken (zoals via internet of internationaal) dergelijke sms'jes te versturen, waarbij ze uiteindelijk ook bij Vodafone klanten terecht kunnen komen.

Spoofing is een algemeen probleem dat al langer bestaat. Deze vorm van sms spoofing is te vergelijken met e-mail spoofing waarbij het lijkt alsof iemand anders de afzender is. Er wordt bij e-mail spoofing ook niet ingebroken in de e-mailbox van de schijnbare afzender.

Technisch gezien is het heel lastig om deze vorm van spoofing te voorkomen. Spoofing sites kunnen namelijk overal ter wereld de sms'jes op het mobiele netwerk brengen waarna het voor andere netwerken met de huidige stand van de techniek moeilijk te verifiëren is of de afzender authentiek is.

311

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 12:32
Aan: [redacted]
Onderwerp: FW: SMS spoofing media coverage

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 12:23
Aan: [redacted]
Onderwerp: SMS spoofing media coverage

Ha[redacted], ik heb je net een voicemail ingesproken nav een item van Powned dat gisteravond op TV was en dat vanavond een vervolg uitzendt. Het gaat hier om een bekend industrie issue en dit is fundamenteel anders dan waar we verleden week mee te maken hadden. We hebben contact gehad met KPN en die hebben dit bevestigd. Zie ook een site als spoever.nl.

[redacted]

[redacted]

Hieronder nog het statement dat wij reactief zullen gebruiken.

Groet
[redacted]

Gisteravond liet Pownews zien dat het mogelijk is om via internet sms-berichten te versturen namens een andere, valse afzender. Dit betreft geen kwetsbaarheid in het mobiele netwerk, ook wordt er niet ingebroken in 'sms-boxen' van gebruikers. Pownews maakte gebruik van een premium (betaalde) sms spoofing dienst die op internet wordt aangeboden. De afzender en ontvanger van de sms kan daarbij zelf ingevuld worden. Met deze dienst wordt de identiteit van iemand anders nagebootst, wat illegaal is. Gebruikers van deze dienst hebben geen toegang tot de sms-berichten van de ogenschijnlijke zender of ontvanger.

Sms spoofing is een internationaal probleem en heeft in Nederland de aandacht van de industrie en overheid/Opta. De aanbieders van sms spoofing diensten versturen sms-berichten vanaf het internet via verschillende mobiele netwerken naar mobiele telefoons. Vodafone Nederland weert aanbieders van dergelijke sms spoofing diensten van zijn netwerk. Echter, dat neemt niet weg dat het mogelijk blijft om via andere netwerken (zoals via internet of internationaal) dergelijke sms'jes te versturen, waarbij ze uiteindelijk ook bij Vodafone klanten terecht kunnen komen.

Spoofing is een algemeen probleem dat al langer bestaat. Deze vorm van sms spoofing is te vergelijken met e-mail spoofing waarbij het lijkt alsof iemand anders de afzender is. Er wordt bij e-mail spoofing ook niet ingebroken in de e-mailbox van de schijnbare afzender.

Technisch gezien is het heel lastig om deze vorm van spoofing te voorkomen. Spoofing sites kunnen namelijk overal ter wereld de sms'jes op het mobiele netwerk brengen waarna het voor andere netwerken met de huidige stand van de techniek moeilijk te verifiëren is of de afzender authentiek is.

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 13:10
Aan: [redacted]
Onderwerp: RE: Commentaar op werkdocument en berichtje over Vodafone voor rijksambtenaren

Hoi,

Vodafone en veilig bellen in den brede krijg je straks een reactie op.

Punten die ik nog had:

[redacted]

Groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:26
Aan: [redacted]
Onderwerp: Commentaar op werkdocument en berichtje over Vodafone voor rijksambtenaren

Dag [redacted]

Kun je mij je commentaar op het werkdocument communicatie uiterlijk maandagochtend mailen? Dank alvast!

En ik wacht even jouw initiatief af voor het Vodafone-traject, goed?

Met vriendelijke groet,

[redacted]
communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 29 maart 2011 17:01
Aan: [redacted]
Onderwerp: berichtje over Vodafone voor rijksambtenaren

Dag [redacted]

In overleg met [redacted]: naar aanleiding van de Vodafone-kwestie het lijkt ons verstandig om de veiligheidsmaatregelen rond telefonie weer eens breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites. Op http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemaildiensten.html is een factsheet gepubliceerd die als basis kan dienen. Als

contactpersoon voor het INIC (Intern Netwerk van Interne Communicatieadviseurs) kan ik het bericht rijksbreed verspreiden.

Ben je het hiermee eens en kan iemand bij jullie op korte termijn het bericht opstellen? Om te voorkomen dat het al te veel als mosterd na de maaltijd komt, zou het deze week uit moeten.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 23 maart 2011 21:42
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: vodafone/ Eén Vandaag

Ter informatie:

[redacted]mma Een Vandaag heeft vanavond aangetoond dat voicemailberichten van vodafone op afstand makkelijk te luisteren waren. Als er geen persoonlijke code was aangemaakt konden berichten afgeluisterd worden via de standaardcode 3333. Alle bewindsleden bellen met vodafone, contract is afgesloten via dgobr. Vodafone heeft inmiddels beveiliging opgeschroeft, op afstand is met standaardcode de voicemail niet meer uit te luisteren. In overleg met AZ, dg obr, en onze minister is een korte wv-lijn opgesteld. Die is aan alle departementen gestuurd. Woordvoering ligt bij ons, behalve inhoud van specifieke voicemailberichten, die ligt bij betreffende departement. Kamer heeft inmiddels opheldering gevraagd. We zullen met DG OBR bespreken welke communicatie wordt ingezet naar alle vodafonegebruikers van het Rijk.

Groet,
[redacted]

Sent with Good (www.good.com)

315

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:00
Aan: [redacted]
Onderwerp: RE: Zoiets qua communicatie?

twee pu.ıtjes

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 13:55
Aan: [redacted]
Onderwerp: Zoiets qua communicatie?

316

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:21
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi [redacted]

Prima idee en prettig dat het INIC voor coördinatie kan zorgen.

Bijgaand een opzetje voor dergelijke communicatie. Het factsheet als link opnemen bij de laatste zin. Hoe naar de brief van Donner moet worden gelinkt, weet ik niet. Hij staat in ieder geval ook hier:
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/03/25/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid.pdf

Ik zou nog wel graag de communicatie-uiting willen zien nadat deze 'onder handen' is genomen en voordat deze richting departementale intranetten gaat.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 29 maart 2011 17:01
Aan: [redacted]
Onderwerp: berichtje over Vodafone voor rijksambtenaren

Dag [redacted]

In overleg met [redacted] naar aanleiding van de Vodafone-kwestie het lijkt ons verstandig om de veiligheidsmaatregelen rond telefonie weer eens breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites. Op http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemaildiensten.html is een factsheet gepubliceerd die als basis kan dienen. Als contactpersoon voor het INIC (Intern Netwerk van Interne Communicatieadviseurs)

kan ik het bericht rijksbreed verspreiden.

Ben je het hiermee eens en kan iemand bij jullie op korte termijn het bericht opstellen? Om te voorkomen dat het al te veel als mosterd na de maaltijd komt, zou het deze week uit moeten.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 23 maart 2011 21:42
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: vodafone/ Eén Vandaag

Ter informatie:

Programma Een Vandaag heeft vanavond aangetoond dat voicemailberichten van vodafone op afstand makkelijk te luisteren waren. Als er geen persoonlijke code was aangemaakt konden berichten afgeluisterd worden via de standaardcode 3333. Alle bewindsleden bellen met vodafone, contract is afgesloten via dgobr. Vodafone heeft inmiddels beveiliging opgeschroeft, op afstand is met standaardcode de voicemail niet meer uit te luisteren. In overleg met AZ, dg obr, en onze minister is een korte wv-lijn opgesteld. Die is aan alle departementen gestuurd. Woordvoering ligt bij ons, behalve inhoud van specifieke voicemailberichten, die ligt bij betreffende departement. Kamer heeft inmiddels opheldering gevraagd. We zullen met DG OBR bespreken welke communicatie wordt ingezet naar alle vodafonegebruikers van het Rijk.

Groet,
[redacted]

Sent with Good (www.good.com)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten Generaal

[redacted]
Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Contactpersoon
[redacted]

Datum 24 maart 2011
Betreft Op afstand afluisteren van mobiele telefoons bij de overheid

In het televisieprogramma Een Vandaag van 23 maart 2011 was te zien hoe op afstand de voicemailberichten konden worden beluisterd van ministers, burgemeesters, kamerleden, topambtenaren en woordvoerders bij de Nederlandse overheid. Op 24 maart 2011 hebben diverse media, waaronder Nieuwsuur en opnieuw Een Vandaag hieraan aandacht besteed. Met deze brief wil ik de Tweede Kamer inlichten over de feiten rond dit ernstig te noemen fenomeen en de genomen maatregelen ter zake.

Een van de diensten die bij mobiele telefonie hoort, is de mogelijkheid om op afstand vanaf een willekeurige telefoon de voicemail van de eigen mobiele telefoon te beluisteren. Om misbruik te voorkomen is dit afluisteren beveiligd met een pincode. Bij Vodafone is deze pincode standaard ingesteld op 3333. De gebruiker kan deze pincode zelf met zijn mobiele telefoon wijzigen in een eigen pincode. Naar nu blijkt had het voicemailsysteem van Vodafone te maken met twee afzonderlijke problemen.

Vodafone had sinds 2007 voor grootzakelijke klanten de mogelijkheid afgeschermd om met deze standaard ingestelde pincode via een willekeurige andere telefoon voicemailberichten op afstand af te luisteren. Echter door een fout bij Vodafone is het sinds november 2010 mogelijk geworden om deze standaard pincode daarvoor wel te gebruiken en is het misbruik dat door Een Vandaag is aangetoond, mogelijk geworden. Vodafone was niet op de hoogte van deze fout totdat Een Vandaag dit publiekelijk maakte. Ook de overheid was van deze fout niet op de hoogte. Vodafone heeft deze fout inmiddels publiekelijk erkend, de verantwoordelijkheid ervoor volledig op zich genomen en ons hun excuses aangeboden. Het genoemde misbruik raakte overigens alle Vodafone abonnees en niet alleen een groot gedeelte van de overheid. De Ministeries van Defensie en voormalig Justitie hebben een andere dienstverlener voor mobiele telefonie en deze voicemailboxen zijn niet door het incident geraakt.

Nadat Een Vandaag melding had gemaakt van de mogelijkheid op genoemde wijze voicemailberichten af te luisteren, heeft Vodafone terstond de fout hersteld. Vodafone heeft ons gemeld dat ze als gevolg van dit incident hun beveiligings- en privacybeleid opnieuw tegen het licht houden.

Het tweede probleem was dat het voicemailsysteem van Vodafone kwetsbaar was voor hetgeen technici 'callerID spoofing' noemen. Dit is een andere, technische meer ingewikkelde methode dan Een Vandaag in het programma van 23 maart heeft getoond. Hierbij stuurt een kwaadwillende een ander afzendernummer mee dan het feitelijke nummer van zijn eigen telefoon. Voor de voicemailcentrale lijkt het dan alsof de gebruiker met de eigen mobiele telefoon toegang wenst tot het voicemailsysteem. Deze methode werkt alleen, indien de gebruiker van de mobiele telefoon niet heeft aangegeven dat er een pincode nodig is voor het beluisteren van de voicemail via de eigen mobiele telefoon. Nieuwsuur heeft op 24 maart aandacht besteed aan deze vorm van identiteitsfraude. Dit probleem is door GovCERT eerder onder de aandacht gebracht van de beveiligingsambtenaren en de (operationele) informatiebeveiligers van alle ministeries en hoge colleges van staat zodat deze op hun beurt gebruikers op de hoogte konden stellen van ter zake passende maatregelen. Helaas moet ik constateren dat dit niet in alle gevallen is gebeurd. Het kabinet heeft eerder al besloten meer centraal te sturen op de ICT-veiligheid door in het kader van uitvoeringsprogramma Compacte Rijksdienst bij het ministerie van Veiligheid en Justitie een ICT-beveiligingsorganisatie in te richten.

Ook Vodafone was eerder op de hoogte van dit probleem en heeft gisteren deze kwetsbaarheid in hun voicemailsysteem opgelost. Deze geconstateerde kwetsbaarheid is in strijd met het contract dat met Vodafone is afgesloten dat te allen tijde voorziet in externe veilige toegang tot de voicemail door middel van een pincode.

Als gevolg van dit incident laat ik voor zover nog mogelijk, onderzoeken of er misbruik is gemaakt van deze fout en, indien daartoe aanleiding bestaat, in hoeverre staatsveiligheid in het geding is geweest. Voorts laat ik onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal ik betrekken bij het inrichten van de ICT-beveiligingsorganisatie.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.P.H. Donner

319

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 15:55
Aan: [redacted]
Onderwerp: RE: maatregelen veilig bellen

Hoi,

Weet je hier al meer over?

Ligt er al een verzoek bij bureau SG oid?

Groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:42
Aan: [redacted]
Onderwerp: FW: maatregelen veilig bellen

Bij jou bekend?

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag |
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 11:32
Aan: [redacted]
CC: [redacted]
Onderwerp: maatregelen veilig bellen

Hoi [redacted]

Ik hoorde dat de Kamercommissie BZK heeft gevraagd om op het punt 'op afstand aflusiten van mobiele telefoons bij de overheid' bewindspersonen worden verzocht de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven. De minister heeft de TK-leden verzocht uiterlijk

do. 31 maart 16 u aanvullende onderwerpen aan te leveren over beveiliging communicatiemiddelen.

Denk dat jij de lead daarin hebt? Ik ben er graag bij betrokken.

Met vriendelijke groeten,

[redacted]

320

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 16:13
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Met vriendelijke groet,

mr drs [redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 16:11
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Bij deze.

Groet, [redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Parlementaire Zaken / Bestuurszaken
tel.nr. [redacted]
-----Oorspronkelijk bericht-----

Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:40
Aan: [redacted]
Onderwerp: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Origineel volgt per post.

Commissie BiZa

Aan de minister van
Binnenlandse Zaken en Koninkrijksrelaties
Mr. J.P.H. Donner

Plaats en datum: Den Haag, 1 april 2011
Betreft: Op afstand afluisteren van mobiele telefoons bij de overheid
Ons kenmerk: 32500-VII-91/2011D16997

Geachte heer Donner,

In de procedurevergadering van de vaste commissie voor Binnenlandse Zaken van 31 maart 2011 is gesproken over uw brief inzake het op afstand afluisteren van mobiele telefoons bij de overheid.
De commissie heeft besloten u te verzoeken de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet, en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven.
De commissie ontvangt voorts graag een overzicht van de huidige maatregelen met betrekking tot de beveiliging van data bij de overheid (bijv. e-mailverkeer, data-opslag etc.).

Naar aanleiding van uw brief zijn in de commissie de volgende vraagpunten aan de orde gesteld.
- Monitoring van ICT-systemen binnen de overheid is van groot belang. Heeft de overheid zicht op wat er gebeurt op haar netwerken, waaronder mailsystemen, en kan ze tijdig ingrijpen als er sprake is van een onbewuste hiaat in de beveiliging of een doelbewuste inbreuk op de beveiliging ?
- Goed opdrachtgeverschap. In hoeverre vormt (informatie-)beveiliging een expliciet aandachtspunt bij een aanbesteding? Het grootste risico is dat in een aanbesteding beveiliging niet in de eisen wordt meegenomen. Bij wie is belegd dat (informatie)beveiliging standaard in aanbestedingen wordt meegenomen?
- Het wordt steeds gebruikelijker om eigen apparatuur te mogen gebruiken op het zakelijke netwerk ('bring your own device' beleid). Dit vergt een goede en veilige infrastructuur. Hoe is dit geregeld bij de overheid en hoe verhoudt dit beleid zich tot het initiatief van enkele ministers om eigen toestellen te gebruiken tegen het advies van de departementale ICT-afdeling in?
- Om succesvol het nieuwe werken te kunnen invoeren in een organisatie is goede en veilige infrastructuur nodig. Hoe is dit geregeld bij de overheid?
- Eigen verantwoordelijkheid. Gebruikers hebben een eigen verantwoordelijkheid bij het veilig gebruiken van communicatiemiddelen en ICT. Hoe wordt dit veilige gebruik binnen de overheid gestimuleerd?
- Het GovCERT en het NBV hebben een taak om de overheid te adviseren en waarschuwen als er mogelijke beveiligingsrisico's zijn. Hebben zij ook een signalerende rol naar de leverancier van producten en diensten, waarin zij dit risico signaleren?

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

Bij deze breng ik u het verzoek en de vragen van de commissie over.

[redacted]

[redacted]

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

Informatie uit de Tweede Kamer gecombineerd met achtergronddossiers en het laatste politieke nieuws.
Informatie ter oriëntatie op een bezoek, uitleg over hoe wetten tot stand komen en een rondgang door de geschiedenis van de Staten-Generaal.
Kijk nu op www.tweedekamer.nl

Disclaimer

Indien u de link niet kunt openen, neemt u dan contact op met telefoonnummer 070-3182211. Meer informatie vindt u op de website www.tweedekamer.nl

If you are unable to access the link, please dial +31 70 3182211.
Additional information is available on the website www.tweedekamer.nl and www.houseofrepresentatives.nl

323

[redacted]

Van: [redacted]
Verzonden: vrijdag 1 april 2011 17:09
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Terugkoppeling [redacted] vanochtend

Beste [redacted]

We hebben met het INIC (Intern Netwerk van Interne Communicatieadviseurs) contact om veiligheidsmaatregelen rond telefonie snel breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites.

We hebben een kort opzetje gemaakt dat door hen zal worden omgezet in een communicabel bericht dat we voor plaatsing nog onder ogen krijgen en dan met jullie willen delen.

Nadien hebben we meer tijd/gelegenheid om een degelijke communicatiestrategie te bedenken voor dit type onderwerpen.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
T [redacted]
[redacted]
http://www.minbzk.nl

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 31 maart 2011 15:01
Aan: [redacted]
CC: [redacted]
Onderwerp: Terugkoppeling [redacted] vanochtend

Beste allemaal,

Nav vanochtend zet ik nog even een aantal dingen op een rij wat betreft de agenda voor de [redacted] van 13 april.

In de bijlage staat een nieuwe versie van de agenda, hier kunnen jullie tot dinsdag 17:00 aanvullingen op doen.

Verder de volgende actiepunten in volgorde van de agenda:
Actie [redacted]t: zin aanleveren voor verslag 16 feb bij [redacted]
Actie [redacted]: actielijst Gateway aanleveren bij [redacted] (na afstemming met vz stuurgroep)

Actie [redacted] actie & besluitenlijst ipv/ aanvullend op verslag
Actie [redacted] check punten Defensie aangaande rijksbrede bev incidenten
Actie [redacted] context plaatsen bij schema inrichting bev functie en vertaalslag van plaat 16 maart naar huidige plaat
Actie [redacted] aanbiedingsformulier zonering met daarin specifieke punten voor CBIB
Actie [redacted] informatie 'Information rights management' rondmailen aan CBIB. Obv daarvan kijken of en hoe verder.
Actie [redacted] Proces stukje over (on) veilige telefonie
Actie [redacted] orgen dat portfeuillehouders stukje aanleveren in juiste format
Actie [redacted] contact opnemen met [redacted] over de leidraad
Actie [redacted] rond thema awareness coordinatie proberen te organiseren
Actie [redacted] onderwerp awareness bespreken in communicatie overleg DGOBR
Actie [redacted] VIR-GI en BIR aan de agenda toevoegen

Graag je actie oppakken en aan mij terugkoppelen indien nodig. Woensdagochtend 6 april verzend ik de stukken.
Alvast hartelijk dank voor jullie bijdragen.

Met vriendelijke groet,

[redacted]
DG Organisatie en Bedrijfsvoering Rijk

[redacted]

Met vriendelijke groet,

[redacted]
DG Organisatie en Bedrijfsvoering Rijk

[redacted]

326

[redacted]

Van: [redacted]
Verzonden: zondag 3 april 2011 23:48
Aan: [redacted]
Onderwerp: Vodafone onderzoeksvragen

Vodafone
nderzoeksvragen.do

327

[redacted]

Van: [redacted]
Verzonden: maandag 4 april 2011 9:36
Aan: [redacted]
Onderwerp: vragen commissie Biza

[redacted]

afgelopen vrijdag(avond) [redacted] nog even gesproken over de vragen van de cie Biza.
[redacted]

Met vriendelijke groet,

[redacted]
Coördinerend senior beleidsmedewerker .....
Ministerie van BZK/DGOBR/ [redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag .....
[redacted]
T [redacted]
[redacted]
http://www.rijksoverheid.nl

328

[redacted]

Van: [redacted]
Verzonden: maandag 4 april 2011 13:28
Aan: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Beste [redacted]

Dank voor je voorzet. Ik stuur hem ongewijzigd door. Het is aan de intranetredacties zelf hier een vertaalverslag in te maken.

Met vriendelijke groet,

[redacted]
communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:21
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi [redacted]

Prima idee en prettig dat het INIC voor coördinatie kan zorgen.

Bijgaand een opzetje voor dergelijke communicatie. Het factsheet als link opnemen bij de laatste zin. Hoe naar de brief van Donner moet worden gelinkt, weet ik niet. Hij staat in ieder geval ook hier:
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/03/25/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid.pdf

Ik zou nog wel graag de communicatie-uiting willen zien nadat deze 'onder handen' is genomen en voordat deze richting departementale intranetten gaat.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 29 maart 2011 17:01
Aan: [redacted]
Onderwerp: berichtje over Vodafone voor rijksambtenaren

Dag [redacted]

In overleg met [redacted] naar aanleiding van de Vodafone-kwestie het lijkt ons verstandig om de veiligheidsmaatregelen rond telefonie weer eens breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites. Op http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemaildiensten.html is een factsheet gepubliceerd die als basis kan dienen. Als contactpersoon voor het INIC (Intern Netwerk van Interne Communicatieadviseurs) kan ik het bericht rijksbreed verspreiden.

Ben je het hiermee eens en kan iemand bij jullie op korte termijn het bericht opstellen? Om te voorkomen dat het al te veel als mosterd na de maaltijd komt, zou het deze week uit moeten.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 23 maart 2011 21:42
Aan: [redacted]
CC: [redacted]
Loek
Onderwerp: FW: vodafone/ Eén Vandaag

Ter informatie:

Programma Een Vandaag heeft vanavond aangetoond dat voicemailberichten van vodafone op afstand makkelijk te luisteren waren. Als er geen persoonlijke code was aangemaakt konden berichten afgeluisterd worden via de standaardcode 3333. Alle bewindsleden bellen met vodafone, contract is afgesloten via dgobr. Vodafone heeft inmiddels beveiliging opgeschroeft, op afstand is met standaardcode de voicemail niet meer uit te luisteren. In overleg met AZ, dg obr, en onze minister is een korte wv-lijn opgesteld. Die is aan alle departementen gestuurd. Woordvoering ligt bij ons, behalve inhoud van specifieke voicemailberichten, die ligt bij betreffende departement. Kamer heeft inmiddels opheldering gevraagd. We zullen met DG OBR bespreken welke communicatie wordt ingezet naar alle vodafonegebruikers van het Rijk.

Groet,
[redacted]

Sent with Good (www.good.com)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten Generaal

DGOBR/DIR

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Contactpersoon
[redacted]

Datum 24 maart 2011
Betreft Op afstand afluisteren van mobiele telefoons bij de overheid

In het televisieprogramma Een Vandaag van 23 maart 2011 was te zien hoe op afstand de voicemailberichten konden worden beluisterd van ministers, burgemeesters, kamerleden, topambtenaren en woordvoerders bij de Nederlandse overheid. Op 24 maart 2011 hebben diverse media, waaronder Nieuwsuur en opnieuw Een Vandaag hieraan aandacht besteed. Met deze brief wil ik de Tweede Kamer inlichten over de feiten rond dit ernstig te noemen fenomeen en de genomen maatregelen ter zake.

Een van de diensten die bij mobiele telefonie hoort, is de mogelijkheid om op afstand vanaf een willekeurige telefoon de voicemail van de eigen mobiele telefoon te beluisteren. Om misbruik te voorkomen is dit afluisteren beveiligd met een pincode. Bij Vodafone is deze pincode standaard ingesteld op 3333. De gebruiker kan deze pincode zelf met zijn mobiele telefoon wijzigen in een eigen pincode. Naar nu blijkt had het voicemailsysteem van Vodafone te maken met twee afzonderlijke problemen.

Vodafone had sinds 2007 voor grootzakelijke klanten de mogelijkheid afgeschermd om met deze standaard ingestelde pincode via een willekeurige andere telefoon voicemailberichten op afstand af te luisteren. Echter door een fout bij Vodafone is het sinds november 2010 mogelijk geworden om deze standaard pincode daarvoor wel te gebruiken en is het misbruik dat door Een Vandaag is aangetoond, mogelijk geworden. Vodafone was niet op de hoogte van deze fout totdat Een Vandaag dit publiekelijk maakte. Ook de overheid was van deze fout niet op de hoogte. Vodafone heeft deze fout inmiddels publiekelijk erkend, de verantwoordelijkheid ervoor volledig op zich genomen en ons hun excuses aangeboden. Het genoemde misbruik raakte overigens alle Vodafone abonnees en niet alleen een groot gedeelte van de overheid. De Ministeries van Defensie en voormalig Justitie hebben een andere dienstverlener voor mobiele telefonie en deze voicemailboxen zijn niet door het incident geraakt.

Nadat Een Vandaag melding had gemaakt van de mogelijkheid op genoemde wijze voicemailberichten af te luisteren, heeft Vodafone terstond de fout hersteld. Vodafone heeft ons gemeld dat ze als gevolg van dit incident hun beveiligings- en privacybeleid opnieuw tegen het licht houden.

Het tweede probleem was dat het voicemailsysteem van Vodafone kwetsbaar was voor hetgeen technici 'callerID spoofing' noemen. Dit is een andere, technische meer ingewikkelde methode dan Een Vandaag in het programma van 23 maart heeft getoond. Hierbij stuurt een kwaadwillende een ander afzendernummer mee dan het feitelijke nummer van zijn eigen telefoon. Voor de voicemailcentrale lijkt het dan alsof de gebruiker met de eigen mobiele telefoon toegang wenst tot het voicemailsysteem. Deze methode werkt alleen, indien de gebruiker van de mobiele telefoon niet heeft aangegeven dat er een pincode nodig is voor het beluisteren van de voicemail via de eigen mobiele telefoon. Nieuwsuur heeft op 24 maart aandacht besteed aan deze vorm van identiteitsfraude. Dit probleem is door GovCERT eerder onder de aandacht gebracht van de beveiligingsambtenaren en de (operationele) informatiebeveiligers van alle ministeries en hoge colleges van staat zodat deze op hun beurt gebruikers op de hoogte konden stellen van ter zake passende maatregelen. Helaas moet ik constateren dat dit niet in alle gevallen is gebeurd. Het kabinet heeft eerder al besloten meer centraal te sturen op de ICT-veiligheid door in het kader van uitvoeringsprogramma Compacte Rijksdienst bij het ministerie van Veiligheid en Justitie een ICT-beveiligingsorganisatie in te richten.

Ook Vodafone was eerder op de hoogte van dit probleem en heeft gisteren deze kwetsbaarheid in hun voicemailsysteem opgelost. Deze geconstateerde kwetsbaarheid is in strijd met het contract dat met Vodafone is afgesloten dat te allen tijde voorziet in externe veilige toegang tot de voicemail door middel van een pincode.

Als gevolg van dit incident laat ik voor zover nog mogelijk, onderzoeken of er misbruik is gemaakt van deze fout en, indien daartoe aanleiding bestaat, in hoeverre staatsveiligheid in het geding is geweest. Voorts laat ik onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal ik betrekken bij het inrichten van de ICT-beveiligingsorganisatie.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.P.H. Donner

329

[redacted]

Van: [redacted]
Verzonden: maandag 4 april 2011 14:14
Aan: [redacted]
CC: [redacted]
Onderwerp: veilig telefoneren

Beste rijkscollega's,

Mogelijk hebben jullie erover gelezen of gehoord in de media: EenVandaag onthulde vorige week woensdag dat het heel eenvoudig is om op afstand Vodafone-voicemails af te luisteren. Als er geen persoonlijke code was aangemaakt, konden berichten via de standaardcode 3333 worden afgeluisterd. Bijna alle departementen hebben een contract met Vodafone dus de voicemails van iedereen in het bezit van een mobiele telefoon van het werk, konden eenvoudig worden afgeluisterd.

Inmiddels heeft Vodafone de beveiliging opgeschroefd en de voicemail is niet meer met de standaardcode op afstand te beluisteren. Maar het blijft van belang dat medewerkers veilig omgaan met hun werktelefoon. De Vodafone-kwestie is een goede aanleiding om dit weer eens onder de aandacht te brengen. Bijgevoegd [redacted] vat informatie die als basis kan dienen voor jullie interne communicatiemiddelen, bijvoorbeeld een bericht op jullie intranet.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Communicatie
Postbus 20011
2500 EA Den Haag

T: [redacted]
F: [redacted]

Ministerie van Veiligheid en Justitie

Govcert.nl

Home > Dienstverlening > Kennis en publicaties > Factsheets

Factsheet over kwetsbaarheden in voicemaildiensten

Laatste wijziging	Fri Mar 25 17:50:00 CET 2011
Eerste publicatie	Thu Mar 24 17:50:42 CET 2011
Versie	1.1
Licentie	Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 3.0 Nederland

Op 23 en 24 maart 2011 is informatie in de media gekomen over twee kwetsbaarheden in de voicemaildienst van Vodafone. Uit eigen tests van GOVCERT.NL is gebleken dat beide kwetsbaarheden inmiddels zijn verholpen door Vodafone.

De belangrijkste feiten op een rij

- Er zijn kwetsbaarheden bekend gemaakt in de voicemaildienst van Vodafone.
- Deze factsheet is ook relevant voor klanten van andere telecomproviders.

Ons advies:

- Gebruik nooit de standaard pincode. Stel altijd een eigen pincode in.
- Laat, indien mogelijk, altijd om een pincode vragen. Ook als u vanaf uw eigen mobiele telefoon uw voicemail beluistert.

Download

- **Factsheet over kwetsbaarheden in voicemaildiensten**
  PDF, klik op de titel om te openen | 43.6220703125 kB

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten Generaal

[redacted]
Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Contactpersoon
[redacted]
[redacted]

Datum 24 maart 2011
Betreft Op afstand afluisteren van mobiele telefoons bij de overheid

In het televisieprogramma Een Vandaag van 23 maart 2011 was te zien hoe op afstand de voicemailberichten konden worden beluisterd van ministers, burgemeesters, kamerleden, topambtenaren en woordvoerders bij de Nederlandse overheid. Op 24 maart 2011 hebben diverse media, waaronder Nieuwsuur en opnieuw Een Vandaag hieraan aandacht besteed. Met deze brief wil ik de Tweede Kamer inlichten over de feiten rond dit ernstig te noemen fenomeen en de genomen maatregelen ter zake.

Een van de diensten die bij mobiele telefonie hoort, is de mogelijkheid om op afstand vanaf een willekeurige telefoon de voicemail van de eigen mobiele telefoon te beluisteren. Om misbruik te voorkomen is dit afluisteren beveiligd met een pincode. Bij Vodafone is deze pincode standaard ingesteld op 3333. De gebruiker kan deze pincode zelf met zijn mobiele telefoon wijzigen in een eigen pincode. Naar nu blijkt had het voicemailsysteem van Vodafone te maken met twee afzonderlijke problemen.

Vodafone had sinds 2007 voor grootzakelijke klanten de mogelijkheid afgeschermd om met deze standaard ingestelde pincode via een willekeurige andere telefoon voicemailberichten op afstand af te luisteren. Echter door een fout bij Vodafone is het sinds november 2010 mogelijk geworden om deze standaard pincode daarvoor wel te gebruiken en is het misbruik dat door Een Vandaag is aangetoond, mogelijk geworden. Vodafone was niet op de hoogte van deze fout totdat Een Vandaag dit publiekelijk maakte. Ook de overheid was van deze fout niet op de hoogte. Vodafone heeft deze fout inmiddels publiekelijk erkend, de verantwoordelijkheid ervoor volledig op zich genomen en ons hun excuses aangeboden. Het genoemde misbruik raakte overigens alle Vodafone abonnees en niet alleen een groot gedeelte van de overheid. De Ministeries van Defensie en voormalig Justitie hebben een andere dienstverlener voor mobiele telefonie en deze voicemailboxen zijn niet door het incident geraakt.

Nadat Een Vandaag melding had gemaakt van de mogelijkheid op genoemde wijze voicemailberichten af te luisteren, heeft Vodafone terstond de fout hersteld. Vodafone heeft ons gemeld dat ze als gevolg van dit incident hun beveiligings- en privacybeleid opnieuw tegen het licht houden.

Het tweede probleem was dat het voicemailsysteem van Vodafone kwetsbaar was voor hetgeen technici 'callerID spoofing' noemen. Dit is een andere, technische meer ingewikkelde methode dan Een Vandaag in het programma van 23 maart heeft getoond. Hierbij stuurt een kwaadwillende een ander afzendernummer mee dan het feitelijke nummer van zijn eigen telefoon. Voor de voicemailcentrale lijkt het dan alsof de gebruiker met de eigen mobiele telefoon toegang wenst tot het voicemailsysteem. Deze methode werkt alleen, indien de gebruiker van de mobiele telefoon niet heeft aangegeven dat er een pincode nodig is voor het beluisteren van de voicemail via de eigen mobiele telefoon. Nieuwsuur heeft op 24 maart aandacht besteed aan deze vorm van identiteitsfraude. Dit probleem is door GovCERT eerder onder de aandacht gebracht van de beveiligingsambtenaren en de (operationele) informatiebeveiligers van alle ministeries en hoge colleges van staat zodat deze op hun beurt gebruikers op de hoogte konden stellen van ter zake passende maatregelen. Helaas moet ik constateren dat dit niet in alle gevallen is gebeurd. Het kabinet heeft eerder al besloten meer centraal te sturen op de ICT-veiligheid door in het kader van uitvoeringsprogramma Compacte Rijksdienst bij het ministerie van Veiligheid en Justitie een ICT-beveiligingsorganisatie in te richten.

Ook Vodafone was eerder op de hoogte van dit probleem en heeft gisteren deze kwetsbaarheid in hun voicemailsysteem opgelost. Deze geconstateerde kwetsbaarheid is in strijd met het contract dat met Vodafone is afgesloten dat te allen tijde voorziet in externe veilige toegang tot de voicemail door middel van een pincode.

Als gevolg van dit incident laat ik voor zover nog mogelijk, onderzoeken of er misbruik is gemaakt van deze fout en, indien daartoe aanleiding bestaat, in hoeverre staatsveiligheid in het geding is geweest. Voorts laat ik onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal ik betrekken bij het inrichten van de ICT-beveiligingsorganisatie.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.P.H. Donner

330

[redacted]

Van: [redacted]
Verzonden: maandag 4 april 2011 15:29
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: veilig telefoneren

Ter informatie.

Met vriendelijke groet,

[redacted]
communicatieadviseur
-----Oorspronkelijk bericht-----
Van [redacted]
Verzonden: maandag 4 april 2011 15:05
Aan: [redacted]
Onderwerp: RE: veilig telefoneren

Dankjewel [redacted]. Wij hebben intern [redacted] afgelopen week aandacht aan het onderwerp besteed. We zullen daar deze informatie aan koppelen.
Met vriendelijke groet,
[redacted]
Senior Communicatieadviseur

Directie Communicatie
Communicatieadvies en Onderzoek
Ministerie van Sociale Zaken en Werkgelegenheid
Anna van Hannoverstraat 4 | 2595BJ | Den Haag | [redacted]
Postbus 90801 | 2509LV | Den Haag

[redacted]
www.rijksoverheid.nl

Van: [redacted]
Verzonden: maandag 4 april 2011 14:14
Aan: [redacted]

CC: [redacted]
Onderwerp: veilig telefoneren
Beste rijksoollega's,
Mogelijk hebben jullie erover gelezen of gehoord in de media: EenVandaag onthulde vorige week woensdag dat het heel eenvoudig is om op afstand Vodafone-voicemails af te luisteren. Als er geen persoonlijke code was aangemaakt, konden berichten via de standaardcode 3333 worden afgeluisterd. Bijna alle departementen hebben een contract met Vodafone dus de voicemails van iedereen in het bezit van een mobiele telefoon van het werk, konden eenvoudig worden afgeluisterd.
Inmiddels heeft Vodafone de beveiliging opgeschroefd en de voicemail is niet meer met de standaardcode op afstand te beluisteren. Maar het blijft van belang dat medewerkers veilig omgaan met hun werktelefoon. De Vodafone-kwestie is een goede aanleiding om dit weer eens onder de aandacht te brengen. Bijgevoegd namens mijn collega's [redacted] at informatie die als basis kan dienen voor jullie interne communicatiemiddelen, bijvoorbeeld een bericht op jullie [redacted]
Met vriendelijke groet,
[redacted]
senior communicatieadviseur
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Communicatie
Postbus 20011
2500 EA Den Haag
[redacted]

****
Bezoekt u binnenkort een locatie van de Rijksoverheid?

Dan dient u in het bezit te zijn van een geldige Rijkspas of een geldig identiteitsbewijs (paspoort,
nationale identiteitskaart, rijbewijs of vreemdelingendocument). Indien u bij controle geen geldig identiteitsbewijs kunt tonen, wordt de toegang geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.

****
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard dan ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to

inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risk inherent in the electronic transmission of messages.
****

331

[redacted]

Van: [redacted]
Verzonden: maandag 4 april 2011 17:55
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Zo staat het nu op ons eigen intranet: http://bzk-intranet/nieuws/default.asp?bericht_id=20226

Met vriendelijke groet,

[redacted]
communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:21
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi [redacted]

Prima idee en prettig dat het INIC voor coördinatie kan zorgen.

Bijgaand een opzetje voor dergelijke communicatie. Het factsheet als link opnemen bij de laatste zin. Hoe naar de brief van Donner moet worden gelinkt, weet ik niet. Hij staat in ieder geval ook hier:
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/03/25/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid.pdf

Ik zou nog wel graag de communicatie-uiting willen zien nadat deze 'onder handen' is genomen en voordat deze richting departementale intranetten gaat.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----

Van: [redacted]
Verzonden: dinsdag 29 maart 2011 17:01
Aan: [redacted]
Onderwerp: berichtje over Vodafone voor rijksambtenaren

Dag [redacted]

In overleg met [redacted] naar aanleiding van de Vodafone-kwestie het lijkt ons verstandig om de veiligheidsmaatregelen rond telefonie weer eens breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites. Op [redacted] is een factsheet gepubliceerd die als basis kan dienen. Als contactpersoon voor het INIC (Intern Netwerk van Interne Communicatieadviseurs) kan ik het bericht rijksbreed verspreiden.

Ben je het hiermee eens en kan iemand bij jullie op korte termijn het bericht opstellen? Om te voorkomen dat het al te veel als mosterd na de maaltijd komt, zou het deze week uit moeten.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 23 maart 2011 21:42
Aan: [redacted]
CC: [redacted]
Loek
Onderwerp: FW: vodafone/ Eén Vandaag

Ter informatie:

Programma Een Vandaag heeft vanavond aangetoond dat voicemailberichten van vodafone op afstand makkelijk te luisteren waren. Als er geen persoonlijke code was aangemaakt konden berichten afgeluisterd worden via de standaardcode 3333. Alle bewindsleden bellen met vodafone, contract is afgesloten via dgobr. Vodafone heeft inmiddels beveiliging opgeschroeft, op afstand is met standaardcode de voicemail niet meer uit te luisteren. In overleg met AZ, dg obr, en onze minister is een korte wv-lijn opgesteld. Die is aan alle departementen gestuurd. Woordvoering ligt bij ons, behalve inhoud van specifieke voicemailberichten, die ligt bij betreffende departement. Kamer heeft inmiddels opheldering gevraagd. We zullen m[redacted] bespreken welke communicatie wordt ingezet naar alle vodafonegebruikers van het Rijk.

Groet,
[redacted]

Sent with Good (www.good.com)

333

[redacted]

Van: [redacted]
Verzonden: dinsdag 5 april 2011 9:49
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi,

Thanx,

Komt hij ook op andere intranetten/rijksportaal?

Groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: maandag 4 april 2011 17:55
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Zo staat het nu op ons eigen intranet: http://bzk-intranet/nieuws/default.asp?bericht_id=20226

Met vriendelijke groet,

[redacted]
communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:21
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi [redacted]

Prima idee en prettig dat het INIC voor coördinatie kan zorgen.

Bijgaand een opzetje voor dergelijke communicatie. Het factsheet als link opnemen bij de laatste zin. Hoe naar de brief van Donner moet worden gelinkt, weet ik niet. Hij staat in ieder geval ook hier:
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/03/25/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid.pdf

Ik zou nog wel graag de communicatie-uiting willen zien nadat deze 'onder handen' is genomen en voordat deze richting departementale intranetten gaat.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
[redacted]
http://www.minbzk.nl

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 29 maart 2011 17:01
Aan: [redacted]
Onderwerp: berichtje over Vodafone voor rijksambtenaren

Dag [redacted]

In overleg met [redacted]: naar aanleiding van de Vodafone-kwestie het lijkt ons verstandig om de veiligheidsmaatregelen rond telefonie weer eens breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites. Op [redacted]s een factsheet gepubliceerd die als basis kan dienen. Als contactpersoon voor het INIC (Intern Netwerk van Interne Communicatieadviseurs) kan ik het bericht rijksbreed verspreiden.

Ben je het hiermee eens en kan iemand bij jullie op korte termijn het bericht opstellen? Om te voorkomen dat het al te veel als mosterd na de maaltijd komt, zou het deze week uit moeten.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 23 maart 2011 21:42
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: vodafone/ Eén Vandaag

Ter informatie:

Programma Een Vandaag heeft vanavond aangetoond dat voicemailberichten van vodafone op afstand makkelijk te luisteren waren. Als er geen persoonlijke code was aangemaakt konden berichten afgeluisterd worden via de standaardcode 3333. Alle bewindsleden bellen met vodafone, contract is afgesloten via dgobr. Vodafone heeft inmiddels beveiliging opgeschroeft, op afstand is met standaardcode de voicemail niet meer uit te luisteren. In overleg met AZ, dg obr, en onze minister is

een korte wv-lijn opgesteld. Die is aan alle departementen gestuurd. Woordvoering ligt bij ons, behalve inhoud van specifieke voicemailberichten, die ligt bij betreffende departement. Kamer heeft inmiddels opheldering gevraagd. We zullen m[redacted]bespreken welke communicatie wordt ingezet naar alle vodafonegebruikers van het Rijk.

Groet,

[redacted]

Sent with Good (www.good.com)

336

[redacted]

Van: [redacted]
Verzonden: dinsdag 5 april 2011 9:53
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Als het goed is wel. Ik heb het tekstje dat [redacted] heeft aangeleverd verspreid onder alle intranetredacties en interne communicatieadviseurs bij het Rijk. Wij kunnen als BZK alleen niets opleggen aan andere departementen, het is aan hen wat en hoe ze intern communiceren. Zie ook de vrijdag besproken communicatiestrategie ;-)

Met vriendelijke groet,

[redacted]
communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 5 april 2011 9:49
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi,

Thanx,

Komt hij ook op andere intranetten/rijksportaal?

Groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: maandag 4 april 2011 17:55
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Zo staat het nu op ons eigen intranet: http://bzk-intranet/nieuws/default.asp?bericht_id=20226

Met vriendelijke groet,

[redacted]
communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:21
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: berichtje over Vodafone voor rijksambtenaren

Hoi [redacted],

Prima idee en prettig dat het INIC voor coördinatie kan zorgen.

Bijgaand een opzetje voor dergelijke communicatie. Het factsheet als link opnemen bij de laatste zin. Hoe naar de brief van Donner moet worden gelinkt, weet ik niet. Hij staat in ieder geval ook hier:
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/03/25/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid/reactie-afluisteren-van-mobiele-telefoons-bij-de-overheid.pdf

Ik zou nog wel graag de communicatie-uiting willen zien nadat deze 'onder handen' is genomen en voordat deze richting departementale intranetten gaat.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag |
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 29 maart 2011 17:01
Aan: [redacted]
Onderwerp: berichtje over Vodafone voor rijksambtenaren

Dag[redacted]

In overleg met [redacted] naar aanleiding van de Vodafone-kwestie het lijkt ons verstandig om de veiligheidsmaatregelen rond telefonie weer eens breed onder de aandacht te brengen bij rijksambtenaren. Bijvoorbeeld door een kort berichtje op Rijksportaal, dat door kan worden geplaatst op de departementale websites. Op [redacted] een factsheet gepubliceerd die als basis kan dienen. Als contactpersoon voor het INIC (Intern Netwerk van Interne Communicatieadviseurs) kan ik het bericht rijksbreed verspreiden.

Ben je het hiermee eens en kan iemand bij jullie op korte termijn het bericht opstellen? Om te voorkomen dat het al te veel als mosterd na de maaltijd komt, zou het deze week uit moeten.

Met vriendelijke groet,

[redacted]
senior communicatieadviseur

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 23 maart 2011 21:42
Aan: [redacted]
CC: [redacted]

Onderwerp: FW: vodafone/ Eén Vandaag

Ter informatie:

Programma Een Vandaag heeft vanavond aangetoond dat voicemailberichten van vodafone op afstand makkelijk te luisteren waren. Als er geen persoonlijke code was aangemaakt konden berichten afgeluisterd worden via de standaardcode 3333. Alle bewindsleden bellen met vodafone, contract is afgesloten via dgobr. Vodafone heeft inmiddels beveiliging opgeschroeft, op afstand is met standaardcode de voicemail niet meer uit te luisteren. In overleg met AZ, dg obr, en onze minister is een korte wv-lijn opgesteld. Die is aan alle departementen gestuurd. Woordvoering ligt bij ons, behalve inhoud van specifieke voicemailberichten, die ligt bij betreffende departement. Kamer heeft inmiddels opheldering gevraagd. We zullen met DG OBR bespreken welke communicatie wordt ingezet naar alle vodafonegebruikers van het Rijk.

Groet,

[redacted]

Sent with Good (www.good.com)

338

[redacted]

Van: [redacted]
Verzonden: dinsdag 5 april 2011 14:55
Aan: [redacted]
Onderwerp: Digidoc bericht: Nieuwe taak voorbereiding spoeddebat Vodafone Voicemailincidenten, afgekeurd

[redacted] is akkoord met de inhoud van de stukken, maar we houden de map tot het debat wordt gehouden. Overigens is het debat van de site van de TK verdwenen. Het dossier is natuurlijk te gebruiken ter voorbereiding van het AO CT op 26/4

Er is een afgekeurde taak binnengekomen in je inbox [redacted]

Klik op voorbereiding spoeddebat Vodafone Voicemailincidenten om de taak te openen.

339

[redacted]

Van: [redacted]
Verzonden: dinsdag 5 april 2011 16:01
Aan: [redacted]
Onderwerp: Nieuwsbrief Bedrijfsvoering Rijk

Kunt u deze nieuwsbrief niet goed lezen? Bekijk dan de online versie. **Nummer 22 / 5 april 2011**

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bedrijfsvoering Rijk
DGOBR, Partner in Bedrijfsvoering

[redacted]

Voorkom kwetsbaarheden in voicemaildiensten

[redacted]

340

[redacted]

Van: [redacted]
Verzonden: donderdag 7 april 2011 16:01
Aan: [redacted]
Onderwerp: Vodafone onderzoeksvragen

Beste [redacted]

hierbij een eerste opzet met vragen voor het onderzoek naar het inbellen op voicemailboxen onder het OT 2010 contract.
[redacted] kan hiermee doorgaan.

Met vriendelijke groet,

[redacted]
Coördinerend senior beleidsmedewerker .....
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag .....
M 06-48100081
T [redacted]
http://www.rijksoverheid.nl

Voorkom kwetsbaarheden in voicemaildiensten

Op 23 en 24 maart 2011 is informatie in de media gekomen over het afluisteren van de Vodafone voicemaildienst van derden. Uit eigen tests van GOVCERT.NL: *Computer Emergency Response Team van de Nederlandse overheid,* blijkt dat de kwetsbaarheden inmiddels zijn verholpen door Vodafone. Wat was er precies aan de hand en wat kun je zelf doen om eventuele problemen te voorkomen?

Wat was er aan de hand?
1. Onjuist gebruik van een standaard pincode.
2. Authenticiteit, uitsluitend op basis van caller-ID (het nummer waarmee gebeld wordt).

Onjuist gebruik van een standaard pincode
De eerste kwetsbaarheid, die op 23 maart publiek is geworden, hield in dat voicemailboxen van klanten van Vodafone voor derden toegankelijk waren, na het ingeven van een mobiel nummer en standaard pincode. Dit betrof die klanten die hun standaard pincode (bij Vodafone 3333) niet gewijzigd hadden in een eigen, persoonlijke pincode.

Authenticatie uitsluitend op basis van caller-ID
De tweede kwetsbaarheid, die op 24 maart publiek is geworden, is het gevolg van het feit dat authenticatie voor de voicemaildienst van Vodafone uitsluitend gebeurde op basis van het caller-ID. Vodafone stelt op basis van het caller-ID vast wie er belt en welke voicemailbox daarbij hoort. Er bestaan echter diensten waarmee men het caller-ID kan spoofen: dit houdt in dat elk willekeurig caller-ID gebruikt kan worden. Dit kan bijvoorbeeld met Skype of online diensten als spoofcard.com. Feitelijk kan iedereen zich hiermee voordoen als een ander en diens voicemail afluisteren zonder dat er om een pincode wordt gevraagd.

Wat is een goede pincode?
Volgens GOVCERT.nl is een pincode goed als je hem gemakkelijk kunt onthouden en een ander hem moeilijk kan raden.
Hieronder een korte opsomming van een combinatie van getallen die GOVCERT afraadt als pincode:

Een standaard pincode (code die je niet zelf hebt gekozen);
- Geboortedata van jezelf of familie;
- Postcodes van woning of werk;
- Cijferreeksen, zoals 1234;
- Volledige herhalingen, zoals 1111.

Meer informatie:
info@govcert.nl of telefonisch via 070-8887555.

343

[redacted]

Van: [redacted]
Verzonden: donderdag 7 april 2011 17:03
Aan: [redacted]
CC: [redacted]
Onderwerp: Vodafone

Hoi [redacted]

Ik heb het document va[redacted]genomen en enkele aanpassingen gedaan. (Zie bijlage met redactie.)
Hieronder een voorstelmail.

[redacted]

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag |[redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
[redacted]
http://www.minbzk.nl
.....

345

[redacted]

Van: [redacted]
Verzonden: donderdag 7 april 2011 20:05
Aan: [redacted]
CC: [redacted]
Onderwerp: onderzoek

Beste [redacted]

We hebben op donderdag 24 maart afgesproken dat Vodafone een snaphot zou maken van de gegevens met betrekking tot het op afstand beluisteren van de voicemail.
In opvolging hierop willen we een eerste stap zetten door een getalsmatig beeld te krijgen van het op afstand beluisteren, zonder dat daar specifieke nummers en dus privacy aspecten mee in het geding zijn.
Daarvoor hebben we een aantal vragen opgesteld die je hieronder aantreft. Graag zouden we binnen een week antwoord verkrijgen op onderstaande vragen zodat er nog tijd is om zo mogelijk vervolgstappen te kunnen (laten) zetten.

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

2. De tweede reeks vragen heeft als doel de omvang van het gebruik vast te stellen van het beluisteren van een voicemailbox via internet (mogelijk spoofing) en is puur getalsmatig.
a. Hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende bronnen zijn de voicemailboxen van OT 2010 nummers gebeld via internet (spoofing) en hoe vaak is dat gedaan (aantal per telefoonnummer)?

Alvast bedankt en

Met vriendelijke groet,

[redacted]

Informatiseringsbeleid Rijk
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schedeldoekshaven 200 | 2511 EZ | Den Haag | Kamer [redacted]
Postbus 20011 | 2500 EA | Den Haag

T +[redacted]
M M +[redacted]

http://www.rijksoverheid.nl/ministeries/bzk

348

[redacted]

Van: [redacted]
Verzonden: vrijdag 8 april 2011 8:27
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: onderzoek

Beste [redacted]

De data zijn inderdaad bewaard. Zoals besproken moeten we bekijken wat we mogen doen binnen de grenzen van de privacy wetgeving.

Ik zal deze vragen met ons Legal team bespreken en daar op terugkomen.

Vriendelijke groet
[redacted]

From: [redacted]
Sent: donderdag 7 april 2011 20:05
To: [redacted]
Cc: [redacted]
Subject: onderzoek

Beste [redacted]

We hebben op donderdag 24 maart afgesproken dat Vodafone een snaphot zou maken van de gegevens met betrekking tot het op afstand beluisteren van de voicemail.
In opvolging hierop willen we een eerste stap zetten door een getalsmatig beeld te krijgen van het op afstand beluisteren, zonder dat daar specifieke nummers en dus privacy aspecten mee in het geding zijn.
Daarvoor hebben we een aantal vragen opgesteld die je hieronder aantreft. Graag zouden we binnen een week antwoord verkrijgen op onderstaande vragen zodat er nog tijd is om zo mogelijk vervolgstappen te kunnen (laten) zetten.

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

2. De tweede reeks vragen heeft als doel de omvang van het gebruik vast te stellen van het beluisteren van een voicemailbox via internet (mogelijk spoofing) en is puur getalsmatig.
a. Hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende bronnen zijn de voicemailboxen van OT 2010 nummers gebeld via internet (spoofing) en hoe vaak is dat gedaan (aantal per telefoonnummer)?

Alvast bedankt en

Met vriendelijke groet,

[redacted]

Informatiseringsbeleid Rijk
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schedeldoekshaven 200 | 2511 EZ | Den Haag | Kamer [redacted]
Postbus 20011 | 2500 EA | Den Haag

T [redacted]
M [redacted]
[redacted]
http://www.rijksoverheid.nl/ministeries/bzk

351

[redacted]

Van: [redacted]
Verzonden: vrijdag 8 april 2011 15:47
Aan: [redacted]
Onderwerp: ICCIO weekbericht week 14

week 14, 8 april 2011

[redacted]

ICCIO weekbericht
week 14, 8 april 2011

[redacted]

Brief Tweede Kamer afluisteren mobiele telefoons

[redacted]

[redacted]

Terug naar boven

Brief Tweede Kamer afluisteren mobiele telefoons

In het weekbericht van week 12 berichtten we over de problemen met de Voicemail van Vodafone. Minister Donner heeft de Tweede Kamer hierover geïnformeerd door middel van een **brief.** GovCERT heeft zijn **factsheet** over dit onderwerp geactualiseerd.

[redacted]

[redacted]

[redacted]

352

[redacted]

Van: [redacted]
Verzonden: vrijdag 8 april 2011 16:11
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: onderzoek

Beste [redacted]

Dank je.
Wanneer kan ik een reactie verwachten?
Wij willen graag zeer snel de Tweede Kamer kunnen informeren over de omvang etc van het incident.

Met vriendelijke groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 8 april 2011 8:27
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: onderzoek

Beste [redacted]

De data zijn inderdaad bewaard. Zoals besproken moeten we bekijken wat we mogen doen binnen de grenzen van de privacy wetgeving.

Ik zal deze vragen met ons Legal team bespreken en daar op terugkomen.

Vriendelijke groet
[redacted]

From: [redacted]
Sent: donderdag 7 april 2011 20:05
To: [redacted]
Cc: [redacted]
Subject: onderzoek

Beste [redacted]

We hebben op donderdag 24 maart afgesproken dat Vodafone een snaphot zou maken van de gegevens met betrekking tot het op afstand beluisteren van de voicemail.
In opvolging hierop willen we een eerste stap zetten door een getalsmatig beeld te krijgen van het op afstand beluisteren, zonder dat daar specifieke nummers en dus privacy aspecten mee in het geding zijn.
Daarvoor hebben we een aantal vragen opgesteld die je hieronder aantreft. Graag zouden we binnen een week antwoord verkrijgen op onderstaande vragen zodat er nog tijd is om zo mogelijk vervolgstappen te kunnen (laten) zetten.

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

2. De tweede reeks vragen heeft als doel de omvang van het gebruik vast te stellen van het beluisteren van een voicemailbox via internet (mogelijk spoofing) en is puur getalsmatig.
a. Hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende bronnen zijn de voicemailboxen van OT 2010 nummers gebeld via internet (spoofing) en hoe vaak is dat gedaan (aantal per telefoonnummer)?

Alvast bedankt en

Met vriendelijke groet,

[redacted]

Informatiseringsbeleid Rijk
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schedeldoekshaven 200 | 2511 EZ | Den Haag | Kamer [redacted]
Postbus 20011 | 2500 EA | Den Haag

T + [redacted]
M M [redacted]

[redacted]
http://www.rijksoverheid.nl/ministeries/bzk

****
Bezoekt u binnenkort een locatie van de Rijksoverheid?

Dan dient u in het bezit te zijn van een geldige Rijkspas of een geldig identiteitsbewijs (paspoort,
nationale identiteitskaart, rijbewijs of vreemdelingendocument). Indien u bij controle geen geldig identiteitsbewijs kunt tonen, wordt de toegang geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.

****

****

355

[redacted]

Van: [redacted]
Verzonden: maandag 11 april 2011 8:41
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: onderzoek

Beste [redacted]

We zijn hier nu naar aan het kijken. Waarschijnlijk kunnen we over de eerste vraag mbt 3333 meer zeggen aan het eind van de week. Het tweede stuk is een stuk complexer.

[redacted] verantwoordelijk voor Security bij ons zal jullie op de hoogte houden van de voortgang.

Groet
[redacted]

From: [redacted]
Sent: vrijdag 8 april 2011 16:11
To: [redacted]
Cc: [redacted]
Subject: RE: onderzoek

Beste [redacted]

Dank je.
Wanneer kan ik een reactie verwachten?
Wij willen graag zeer snel de Tweede Kamer kunnen informeren over de omvang etc van het incident.

Met vriendelijke groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 8 april 2011 8:27
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: onderzoek

Beste [redacted]

De data zijn inderdaad bewaard. Zoals besproken moeten we bekijken wat we mogen doen binnen de grenzen van de privacy wetgeving.

Ik zal deze vragen met ons Legal team bespreken en daar op terugkomen.

Vriendelijke groet
[redacted]

From: [redacted]
Sent: donderdag 7 april 2011 20:05
To: [redacted]
Cc: [redacted]
Subject: onderzoek

Beste [redacted]

We hebben op donderdag 24 maart afgesproken dat Vodafone een snaphot zou maken van de gegevens met betrekking tot het op afstand beluisteren van de voicemail.
In opvolging hierop willen we een eerste stap zetten door een getalsmatig beeld te krijgen van het op afstand beluisteren, zonder dat daar specifieke nummers en dus privacy aspecten mee in het geding zijn.
Daarvoor hebben we een aantal vragen opgesteld die je hieronder aantreft. Graag zouden we binnen een week antwoord verkrijgen op onderstaande vragen zodat er nog tijd is om zo mogelijk vervolgstappen te kunnen (laten) zetten.

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

2. De tweede reeks vragen heeft als doel de omvang van het gebruik vast te stellen van het beluisteren van een voicemailbox via internet (mogelijk spoofing) en is puur getalsmatig.
a. Hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende bronnen zijn de voicemailboxen van OT 2010 nummers gebeld via internet (spoofing) en hoe vaak is dat gedaan (aantal per telefoonnummer)?

Alvast bedankt en

Met vriendelijke groet,

[redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag

[redacted]

http://www.rijksoverheid.nl/ministeries/bzk

****
Bezoekt u binnenkort een locatie van de Rijksoverheid?

Dan dient u in het bezit te zijn van een geldige Rijkspas of een geldig identiteitsbewijs (paspoort,
nationale identiteitskaart, rijbewijs of vreemdelingendocument). Indien u bij controle
geen geldig identiteitsbewijs kunt tonen, wordt de toegang geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.

****
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de
geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u
verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat
aanvaardt geen aansprakelijkheid voor schade, van welke aard dan ook, die verband
houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not
the addressee or if this message was sent to you by mistake, you are requested to
inform the sender and delete the message. The State accepts no liability for
damage of any kind resulting from the risk inherent in the electronic transmission
of messages.
****

357

[redacted]

Van: [redacted]
Verzonden: maandag 11 april 2011 16:54
Aan: [redacted]
CC: [redacted]
Onderwerp: Betr: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Beste [redacted],

Voor de brief aan de minister mbt 'op afstand afluisteren van mobiele telefoons bij de overheid' hebben we alvast een bijdrage geschreven. Ik denk dat wij vooral kunnen bijdragen op de twee laatste vragen. Weet je al meer over de planning?

Graag blijf ik betrokken. En stuur je met de volledige conceptbrief toe voor akkoord van de leiding hier, aangezien er aanzienlijk deel over de dienst in staat? Net zoals met annotatie voor MR laatst met jullie DG?

Met vriendelijke groeten,

[redacted]

-----[redacted]" <[redacted]schreef: -----

Aan: <[redacted]>
Van: "[redacted]>
Datum: 5-4-2011 10:16
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 16:11

Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Bij deze.

Groet, [redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Parlementaire Zaken / Bestuurszaken
tel.nr. [redacted]
-----Oorspronkelijk bericht-----

Van: Commissie BiZa [mailto:[redacted]]
Verzonden: vrijdag 1 april 2011 14:40
Aan: Parlementaire Zaken BZK; Postbus minBZK
Onderwerp: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Origineel volgt per post.
Informatie uit de Tweede Kamer gecombineerd met achtergronddossiers en het laatste politieke nieuws.
Informatie ter oriÃ«ntatie op een bezoek, uitleg over hoe wetten tot stand komen en een rondgang door de geschiedenis van de Staten-Generaal.
Kijk nu op www.tweedekamer.nl

Disclaimer

Indien u de link niet kunt openen, neemt u dan contact op met telefoonnummer [redacted]. Meer informatie vindt u op de website www.tweedekamer.nl

If you are unable to access the link, please dial [redacted]
Additional information is available on the website www.tweedekamer.nl and www.houseofrepresentatives.nl

[bijlage "b2c2f37d-3fc8-4bcc-a999-1587d6578499.pdf" verwijderd door p3505]
=

358

[redacted]

Van: [redacted]
Verzonden: maandag 11 april 2011 17:01
Aan: [redacted]
CC: [redacted]
Onderwerp: Onderzoek
Urgentie: Hoog
Gevoeligheid: Privé

Beste [redacted]

Naar aanleiding van ons telefoongesprek van vandaag over het voicemail onderzoek wil ik je graag over onze voortgang berichten. Ten aanzien van jullie eerste vraag streven wij ernaar om de antwoorden donderdag a.s. in een met pw beveiligde zip file naar jou toe te mailen. Ten aanzien van de tweede vraag zijn wij geadviseerd dat in verband met de complexiteit van het onderzoek en de analyse van specifieke OT MSISDNs (ook al blijven deze anoniem) niet zonder een bevoegd bevel door ons kan worden beantwoord. Wij spraken af dat jij woensdag a.s. met de bva's zou bezien in hoeverre een dergelijk bevel kan worden uitgevaardigd.

Groet,

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KX Maastricht

Postbus 1500, 6201 BM Maastricht

362

[redacted]

Van: [redacted]
Verzonden: maandag 11 april 2011 18:51
Aan: Alle gebruikers
Onderwerp: Nieuwsbrief intranet 11 april 2011

11 april 2011

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Nieuwsbrief intranet
11 april 2011

[redacted]

Inhoud

[redacted]

Tips voor veilig telefoneren

[redacted]

[redacted]

Lees meer (lees meer voor buitenlocaties)

Terug naar boven

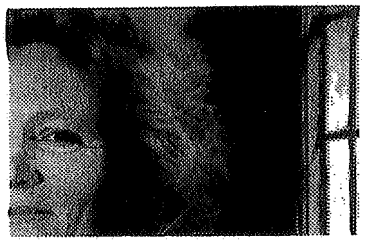
Tips voor veilig telefoneren

Recent is in de media veel aandacht besteed aan het afluisteren van voicemail van Vodafone. Minister Donner heeft de Tweede Kamer hier inmiddels met een brief over geïnformeerd en Vodafone heeft de problemen opgelost. Toch is niet te garanderen dat er niet opnieuw dergelijke of gerelateerde problemen zullen ontstaan. Daarom enkele adviezen.

Lees meer (lees meer voor buitenlocaties)

Terug naar boven

[redacted]



[redacted]

[redacted]

[redacted]

Van: [redacted]
Verzonden: dinsdag 12 april 2011 7:48
Aan: [redacted]
Onderwerp: FW: Onderzoek
Urgentie: Hoog
Gevoeligheid: Privé

collegae, hieronder de stvz naar onderzoek vodafone-incident. Helemaal onderaan onze vragen. Morgen bespreken we in cbib onze tweede vraag. Die ligt een stuk gevoeliger qua privacy.

groet,
[redacted]
-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: maandag 11 april 2011 17:01
Aan: [redacted]
CC: [redacted]
Onderwerp: Onderzoek
Urgentie: Hoog
Gevoeligheid: Privé

Beste [redacted]

Naar aanleiding van ons telefoongesprek van vandaag over het voicemail onderzoek wil ik je graag over onze voortgang berichten. Ten aanzien van jullie eerste vraag streven wij ernaar om de antwoorden donderdag a.s. in een met pw beveiligde zip file naar jou toe te mailen. Ten aanzien van de tweede vraag zijn wij geadviseerd dat in verband met de complexiteit van het onderzoek en de analyse van specifieke OT MSISDNs (ook al blijven deze anoniem) niet zonder een bevoegd bevel door ons kan worden beantwoord. Wij spraken af dat jij woensdag a.s. met de bva's zou bezien in hoeverre een dergelijk bevel kan worden uitgevaardigd.

Groet,

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KX Maastricht

Postbus 1500, 6201 BM Maastricht

We hebben op donderdag 24 maart afgesproken dat Vodafone een snaphot zou maken van de gegevens met betrekking tot het op afstand beluisteren van de voicemail.

In opvolging hierop willen we een eerste stap zetten door een getalsmatig beeld te krijgen van het op afstand beluisteren, zonder dat daar specifieke nummers en dus privacy aspecten mee in het geding zijn.

Daarvoor hebben we een aantal vragen opgesteld die je hieronder aantreft. Graag zouden we binnen een week antwoord verkrijgen op onderstaande vragen zodat er nog tijd is om zo mogelijk vervolgstappen te kunnen (laten) zetten.

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).

a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).

b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).

c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

2. De tweede reeks vragen heeft als doel de omvang van het gebruik vast te stellen van het beluisteren van een voicemailbox via internet (mogelijk spoofing) en is puur getalsmatig.

a. Hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).

b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).

c. Vanaf hoeveel verschillende bronnen zijn de voicemailboxen van OT 2010 nummers gebeld via internet (spoofing) en hoe vaak is dat gedaan (aantal per telefoonnummer)?

364

[redacted]

Van: [redacted]
Verzonden: woensdag 13 april 2011 9:54
Aan: [redacted]
Onderwerp: FW: Onderzoek

Urgentie: Hoog
Gevoeligheid: Privé

Sent with Good (www.good.com)

-----Original Message-----
From: [redacted]
Sent: Monday, April 11, 2011 05:01 PM W. Europe Standard Time
To: [redacted]
Cc: [redacted]
Subject: Onderzoek

Beste [redacted],

Naar aanleiding van ons telefoongesprek van vandaag over het voicemail onderzoek wil ik je graag over onze voortgang berichten. Ten aanzien van jullie eerste vraag streven wij ernaar om de antwoorden donderdag a.s. in een met pw beveiligde zip file naar jou toe te mailen. Ten aanzien van de tweede vraag zijn wij geadviseerd dat in verband met de complexiteit van het onderzoek en de analyse van specifieke OT MSISDNs (ook al blijven deze anoniem) niet zonder een bevoegd bevel door ons kan worden beantwoord. Wij spraken af dat jij woensdag a.s. met de bva's zou bezien in hoeverre een dergelijk bevel kan worden uitgevaardigd.

Groet,

[redacted]

[redacted]

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl <http://www.vodafone.nl/>

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KX Maastricht

Postbus 1500, 6201 BM Maastricht

and do not copy or disclose it or its contents or use it for any purpose. Please also note that transmission cannot be guaranteed to be secure or error-free.

P Please consider the environment before printing this e-mail

366

[redacted]

Van: [redacted]
Verzonden: woensdag 13 april 2011 12:13
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: [IB-list] vodafone voicemail en caller-ID spoofing

Ha[redacted]

Dank voor de brief. Ik las ook de laatste strofe van de brief:
"Voorts laat ik onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal ik betrekken bij de inrichting van de ICT-beveiligingsorganisatie."

Ik heb een paar vragen, omdat dit direct de dienstverlening van mijn team raakt:
- Waar wordt dit onderzoek uitgevoerd en wie gaat dit doen?
- De minister heeft zich niet op een termijn vastgelegd, maar wat schat jij in dat deze is?
- Kunnen wij aanhaken om te kijken of we de signaleringen nog kunnen verbeteren?
- Ik begrijp dat bij de inrichting van de ICT-beveiligingsorganisatie gesproken wordt met Defensie. [redacted] Ik wil hier graag in het voortraject al bij betrokken worden. Ben jij zelf hierbij betrokken of kun jij een contactpersoon [redacted]

Groet,

[redacted]

From: [redacted]
Sent: maandag 28 maart 2011 10:33
To: [redacted]
Subject: [IB-list] vodafone voicemail en caller-ID spoofing

beste collega's,

hierbij zend ik jullie de brief, die onze minister heeft verzonden naar de tweede Kamer over de incidenten met de voicemail.
Uiteraard aanbevolen leeswerk.
Er is sprake van, dat er deze week nog een spoeddebat volgt.

Met vriendelijke groet,

[redacted]

Coördinerend senior beleidsmedewerker
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
[redacted]

http://www.rijksoverheid.nl
Samen met de ministeries optimaliseert en faciliteert DG OBR de bedrijfsvoering en organisatie van het Rijk. Zo kan het Rijk zijn maatschappelijke functie beter vervullen.

307

[redacted]

Van: [redacted]
Verzonden: donderdag 14 april 2011 19:13
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: [IB-list] vodafone voicemail en caller-ID spoofing

[redacted]

ik ga nu met vakantie.
[redacted]

Met vriendelijke groet,

[redacted]
Coördinerend senior beleidsmedewerker
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
[redacted]

http://www.rijksoverheid.nl
Samen met de ministeries optimaliseert en faciliteert DG OSR de bedrijfsvoering en organisatie van het Rijk. Zo kan het Rijk zijn maatschappelijke functie beter vervullen.

----Oorspronkelijk bericht----
Van: [redacted]
Verzonden: woensdag 13 april 2011 12:13
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: [IB-list] vodafone voicemail en caller-ID spoofing

Ha [redacted]

Dank voor de brief. Ik las ook de laatste strofe van de brief:
"Voorts laat ik onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal ik betrekken bij de inrichting van de ICT-beveiligingsorganisatie."

Ik heb een paar vragen, omdat dit direct de dienstverlening van mijn team raakt:
- Waar wordt dit onderzoek uitgevoerd en wie gaat dit doen?
- De minister heeft zich niet op een termijn vastgelegd, maar wat schat jij in dat deze is?
- Kunnen wij aanhaken om te kijken of we de signaleringen nog kunnen verbeteren?
- Ik begrijp dat bij de inrichting van de ICT-beveiligingsorganisatie gesproken wordt met Defensie. [redacted] Ik wil hier graag in het voortraject al bij betrokken worden. Ben jij zelf hierbij betrokken of kun jij een contact regelen?

Groet,

[redacted]

From: [redacted]
Sent: maandag 28 maart 2011 10:33
To: [redacted]
Subject: [IB-list] vodafone voicemail en caller-ID spoofing

beste collega's,

hierbij zend ik jullie de brief, die onze minister heeft verzonden naar de tweede Kamer over de incidenten met de voicemail.
Uiteraard aanbevolen leeswerk.
Er is sprake van, dat er deze week nog een spoeddebat volgt.

Met vriendelijke groet,

[redacted]
Coördinerend senior beleidsmedewerker
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag [redacted]
Postbus 20011 | 2500 EA | Den Haag
T [redacted]

http://www.rijksoverheid.nl
Samen met de ministeries optimaliseert en faciliteert DG OSR de bedrijfsvoering en organisatie van het Rijk. Zo kan het Rijk zijn maatschappelijke functie beter vervullen.

houdt met risico's verbonden aan het elektronisch verzenden van berichten.

3 0 8

[redacted]

Van: [redacted]
Verzonden: donderdag 14 april 2011 23:13
Aan: [redacted]
Onderwerp: RE: Onderzoek

Ik heb het nog niet. Morgen bellen dus. Tweede vraag is complex en vraagt om 11 bevelen. Is misschien niet nodig als duidelijk is dat vraag 1 oplevert dat de omvang beperkt is

Sent with Good (www.good.com)

-----Original Message-----
From: [redacted]
Sent: Thursday, April 14, 2011 11:06 PM W. Europe Standard Time
To: [redacted]
Subject: FW: Onderzoek

Wat is de status?
[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, April 12, 2011 07:47 AM W. Europe Standard Time
To: [redacted]
Subject: FW: Onderzoek

collegae, hieronder de stvz naar onderzoek vodafone-incident. Helemaal onderaan onze vragen. Morgen bespreken we in cbib onze tweede vraag. Die ligt een stuk gevoeliger qua privacy.

groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: maandag 11 april 2011 17:01
Aan: [redacted]
CC: [redacted]
Onderwerp: Onderzoek
Urgentie: Hoog
Gevoeligheid: Privé

Beste [redacted]

Naar aanleiding van ons telefoongesprek van vandaag over het voicemail onderzoek wil ik je graag over onze voortgang berichten. Ten aanzien van jullie eerste vraag streven wij ernaar om de antwoorden donderdag a.s. in een met pw beveiligde zip file naar jou toe te mailen. Ten aanzien van de tweede vraag zijn wij geadviseerd dat in verband met de complexiteit van het onderzoek en de analyse van specifieke OT MSISDNs (ook al blijven deze anoniem) niet zonder een bevoegd bevel door ons kan worden beantwoord. Wij spraken af dat jij woensdag a.s. met de bva's zou bezien in hoeverre een dergelijk bevel kan worden uitgevaardigd.

Groet,

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl <http://www.vodafone.nl/>

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KX Maastricht

Postbus 1500, 6201 BM Maastricht

We hebben op donderdag 24 maart afgesproken dat Vodafone een snaphot zou maken van de cijfers met betrekking tot het op afstand beluisteren van de voicemail.

In opvolging hierop willen we een eerste stap zetten door een getalsmatig beeld te krijgen van het op afstand beluisteren, zonder dat daar specifieke nummers en dus privacy aspecten mee in het geding zijn.

Daarvoor hebben we een aantal vragen opgesteld die je hieronder aantreft. Graag zouden we binnen een week antwoord verkrijgen op onderstaande vragen zodat er nog tijd is om zo mogelijk vervolgstappen te kunnen (laten) zetten.

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).

a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).

b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).

c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

2. De tweede reeks vragen heeft als doel de omvang van het gebruik vast te stellen van het beluisteren van een voicemailbox via internet (mogelijk spoofing) en is puur getalsmatig.

a. Hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).

b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van het beluisteren van een voicemailbox via internet (spoofing)? Graag gespecificeerd naar periode (per week).

c. Vanaf hoeveel verschillende bronnen zijn de voicemailboxen van OT 2010 nummers gebeld via internet (spoofing) en hoe vaak is dat gedaan (aantal per telefoonnummer)?

369

[redacted]

Van: [redacted]
Verzonden: vrijdag 15 april 2011 8:48
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Onderzoek
Gevoeligheid: Privé

Beste [redacted]

Ik heb gisteren niets ontvangen. Kan ik het vandaag wel verwachten?

Alvast bedankt en

Met vriendelijke groet,

[redacted]

Informatiseringsbeleid Rijk
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schedeldoekshaven 200 | 2511 EZ | Den Haag | Kamer [redacted]
Postbus 20011 | 2500 EA | Den Haag

T +[redacted]
M M [redacted]

http://www.rijksoverheid.nl/ministeries/bzk

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: maandag 11 april 2011 17:01
Aan: [redacted]
CC: [redacted]
Onderwerp: Onderzoek
Urgentie: Hoog
Gevoeligheid: Privé

Beste [redacted]

Naar aanleiding van ons telefoongesprek van vandaag over het voicemail onderzoek wil ik je graag over onze voortgang berichten. Ten aanzien van jullie eerste vraag streven wij ernaar om de antwoorden donderdag a.s. in een met pw beveiligde zip file naar jou toe te mailen. Ten aanzien van de tweede vraag zijn wij geadviseerd dat in verband met de complexiteit van het onderzoek en de analyse van specifieke OT MSISDNs (ook al blijven deze anoniem) niet zonder een bevoegd bevel door ons kan worden beantwoord. Wij spraken af dat jij woensdag a.s. met de bva's zou bezien in hoeverre een dergelijk bevel kan worden uitgevaardigd.

Groet,

[redacted]

[redacted]

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KX Maastricht

Postbus 1500, 6201 BM Maastricht

372

[redacted]

Van: [redacted]
Verzonden: vrijdag 15 april 2011 6:53
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Onderzoek
Gevoeligheid: Privé

[redacted] absoluut en zeker; wij leggen er 'as we speak' de laatste hand aan.

From: [redacted]
Sent: vrijdag 15 april 2011 6:48
To: [redacted]
Cc: [redacted]
Subject: RE: Onderzoek
Sensitivity: Private

Beste [redacted]

Ik heb gisteren niets ontvangen. Kan ik het vandaag wel verwachten?

Alvast bedankt en

Met vriendelijke groet,

[redacted]

Informatiseringsbeleid Rijk
DGOBR
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schedeldoekshaven 200 | 2511 EZ | Den Haag | Kame[redacted]
Postbus 20011 | 2500 EA | Den Haag

T +[redacted]
M M +[redacted]
[redacted]
http://www.rijksoverheid.nl/ministeries/bzk

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: maandag 11 april 2011 17:01
Aan: [redacted]
CC: [redacted]
Onderwerp: Onderzoek
Urgentie: Hoog
Gevoeligheid: Privé

Beste [redacted]

Naar aanleiding van ons telefoongesprek van vandaag over het voicemail onderzoek wil ik je graag over onze voortgang berichten. Ten aanzien van jullie eerste vraag streven wij ernaar om de antwoorden donderdag a.s. in een met pw beveiligde zip file naar jou toe te mailen. Ten aanzien van de tweede vraag zijn wij geadviseerd dat in verband met de complexiteit van het onderzoek en de analyse van specifieke OT MSISDNs (ook al blijven deze anoniem) niet zonder een bevoegd bevel door ons kan worden beantwoord. Wij spraken af dat jij woensdag a.s. met de bva's zou bezien in hoeverre een dergelijk bevel kan worden uitgevaardigd.

Groet,

[redacted]
[redacted]
[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KK Maastricht

Postbus 1500, 6201 BM Maastricht

****

Bezoekt u binnenkort een locatie van de Rijksoverheid?

Dan dient u in het bezit te zijn van een geldige Rijkspas of een geldig identiteitsbewijs (paspoort,
nationale identiteitskaart, rijbewijs of vreemdelingendocument). Indien u bij controle geen geldig identiteitsbewijs kunt tonen, wordt de toegang geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.

****

****

375

[redacted]

Van: [redacted]
Verzonden: vrijdag 15 april 2011 10:21
Aan: [redacted]
CC: [redacted]
Onderwerp: [Bericht Encrypted]Onderzoek
Urgentie: Hoog

Beste [redacted]

Bijgaand een met password beveiligde zip file waarin je onze antwoorden op vraag 1 van het voicemail onderzoek zult aantreffen. Password stuur ik je per SMS toe. Als er vragen zijn hoor ik het graag.

<<Voicemail analyse OT2010 v2.zip>>

[redacted]

[redacted]

Tel: [redacted]

E-mail: [redacted]

Web: www.vodafone.nl

Vodafone Netherlands

KvK-nummer 14052264

Avenue Céramique 300, 6221 KX Maastricht

Postbus 1500, 6201 BM Maastricht

Voicemail analyse OT2010

Analyse periode: 01/12/2010 – 23/03/2011

Aantal OT2010 MSISDNs [redacted]
Aantal OT2010 abonnees die in de betreffende periode actief voicemail gebruikt hebben
Aantal OT2010 voicemail berichten dat in de betreffende periode is ingesproken
Aantal keren dat een OT2010 abonnee ingelogd is in zijn voicemail systeem in de betreffende periode
Opmerking: je kunt meerdere voicemail berichten uitluisteren, als je 1 keer inlogt op het voicemail systeem

Vragen OT

1. De eerste vraag heeft als doel de omvang van het gebruik van de standaard pincode 3333 voor het op afstand via een vaste of mobiele telefoon afluisteren van voicemailboxen vast te stellen en is puur getalsmatig (statistisch onderzoek).

a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).

b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).

c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

Vodafone heeft geen historische data van wanneer abonnees wel of niet hun PIN gepersonaliseerd hebben (PIN anders gemaakt hebben dan 3333). Vodafone heeft wel informatie of momenteel de PIN van een abonnee wel of niet gepersonaliseerd is.

Conclusie

Over de periode 01/12/2010 t/m 23/03/2011, 17.45 uur, zijn de totalen als volgt (kort daarna op 23 maart was de uitzending van EenVandaag over Vodafone voicemail):

1a : de voicemail van OT2010 abonnees is [redacted] keer op afstand beluisterd. In deze periode is het niet bekend of de PIN 3333 was of niet.
1b : de voicemail is bij [redacted] OT2010 abonnees op afstand beluisterd. In deze periode is het niet bekend of de PIN 3333 was of niet.
1c : de voicemail van OT2010 abonnees is vanaf [redacted] verschillende MSISDNs op afstand beluisterd. In deze periode is het niet bekend of de PIN 3333 was of niet.

Antwoorden

1a : verstrekte informatie is, hoe vaak op afstand de voicemail beluisterd is van OT2010 abonnees. In de periode t/m 23 maart, 17.45 uur, is het niet bekend of de PIN 3333 was of niet.
1b : verstrekte informatie is, bij hoeveel OT2010 abonnees op afstand de voicemail beluisterd is. In de periode t/m 23 maart, 17.45 uur, is het niet bekend of de PIN 3333 was of niet.
1c : verstrekte informatie is, vanaf hoeveel verschillende MSISDNs op afstand de voicemail beluisterd is van OT2010 abonnees. In de periode t/m 23 maart, 17.45 uur, is het niet bekend of de PIN 3333 was of niet.

week nummer	Vraag 1a	Vraag 1b	Vraag 1c
48			
49			
50			
51			
52			
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12 (ma-wo)			

maandag t/m woensdag 23 maart, 17.45 uur

Weken lopen altijd van maandag t/m zondag, behalve in week 48 = woensdag 1 december t/m zondag 5 december

380

[redacted]

Van: [redacted]
Verzonden: vrijdag 15 april 2011 11:41
Aan: [redacted]
Onderwerp: FW: Nummers

Met vriendelijke groet,

[redacted] *(DGOBR)*
BZK, kamer [redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Bezoekadres: Schedeldoekshaven 200, Den Haag
Postadres: Postbus 20011
2500 EA Den Haag
-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 30 maart 2011 14:00
Aan: [redacted]
Onderwerp: Nummers

Hoi [redacted]

Voor alle zekerheid bijgaande de m.i. relevante nummers. Aangegeven is of er ja/nee een pincode op de voicemail zat voorafgaand aan de commotie (nu bij allemaal, natuurlijk).

Groeten, [redacted]

381

[redacted]

Van: [redacted]
Verzonden: donderdag 21 april 2011 16:24
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 16:11
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Bij deze.

Groet, [redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Parlementaire Zaken / Bestuurszaken
tel.nr. [redacted]
-----Oorspronkelijk bericht-----

Van: Commissie BiZa [redacted]
Verzonden: vrijdag 1 april 2011 14:40
Aan: Parlementaire Zaken BZK; Postbus minBZK
Onderwerp: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Origineel volgt per post.

Commissie BiZa

Aan de minister van
Binnenlandse Zaken en Koninkrijksrelaties
Mr. J.P.H. Donner

Plaats en datum: Den Haag, 1 april 2011
Betreft: Op afstand afluisteren van mobiele telefoons bij de overheid
Ons kenmerk: 32500-VII-91/2011D16997

Geachte heer Donner,

In de procedurevergadering van de vaste commissie voor Binnenlandse Zaken van 31 maart 2011 is gesproken over uw brief inzake het op afstand afluisteren van mobiele telefoons bij de overheid.
De commissie heeft besloten u te verzoeken de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet, en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven.
De commissie ontvangt voorts graag een overzicht van de huidige maatregelen met betrekking tot de beveiliging van data bij de overheid (bijv. e-mailverkeer, data-opslag etc.).

Naar aanleiding van uw brief zijn in de commissie de volgende vraagpunten aan de orde gesteld.
- Monitoring van ICT-systemen binnen de overheid is van groot belang. Heeft de overheid zicht op wat er gebeurt op haar netwerken, waaronder mailsystemen, en kan ze tijdig ingrijpen als er sprake is van een onbewuste hiaat in de beveiliging of een doelbewuste inbreuk op de beveiliging ?
- Goed opdrachtgeverschap. In hoeverre vormt (informatie-)beveiliging een expliciet aandachtspunt bij een aanbesteding? Het grootste risico is dat in een aanbesteding beveiliging niet in de eisen wordt meegenomen. Bij wie is belegd dat (informatie)beveiliging standaard in aanbestedingen wordt meegenomen?
- Het wordt steeds gebruikelijker om eigen apparatuur te mogen gebruiken op het zakelijke netwerk ('bring your own device' beleid). Dit vergt een goede en veilige infrastructuur. Hoe is dit geregeld bij de overheid en hoe verhoudt dit beleid zich tot het initiatief van enkele ministers om eigen toestellen te gebruiken tegen het advies van de departementale ICT-afdeling in?
- Om succesvol het nieuwe werken te kunnen invoeren in een organisatie is goede en veilige infrastructuur nodig. Hoe is dit geregeld bij de overheid?
- Eigen verantwoordelijkheid. Gebruikers hebben een eigen verantwoordelijkheid bij het veilig gebruiken van communicatiemiddelen en ICT. Hoe wordt dit veilige gebruik binnen de overheid gestimuleerd?
- Het GovCERT en het NBV hebben een taak om de overheid te adviseren en waarschuwen als er mogelijke beveiligingsrisico's zijn. Hebben zij ook een signalerende rol naar de leverancier van producten en diensten, waarin zij dit risico signaleren?

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

Bij deze breng ik u het verzoek en de vragen van de commissie over.

[redacted]

[redacted]

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

Informatie uit de Tweede Kamer gecombineerd met achtergronddossiers en het laatste politieke nieuws.
Informatie ter oriëntatie op een bezoek, uitleg over hoe wetten tot stand komen en een rondgang door de geschiedenis van de Staten-Generaal.
Kijk nu op www.tweedekamer.nl

Disclaimer

Indien u de link niet kunt openen, neemt u dan contact op met telefoonnummer 070-3182211. Meer informatie vindt u op de website www.tweedekamer.nl

If you are unable to access the link, please dial +31 70 3182211.
Additional information is available on the website www.tweedekamer.nl and www.houseofrepresentatives.nl

382

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 april 2011 10:50
Aan: [redacted]
Onderwerp: RE: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

De pdf is een brief die de cie BZK van de Kamer naar minister Donner stuurde nav het Vodafone-incident.

[redacted]

[redacted]kun jij ook de feitelijke vragen nog aanvullen?

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 21 april 2011 16:24
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 16:11
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Bij deze.

Groet, [redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Parlementaire Zaken / Bestuurszaken
tel.nr [redacted]

-----Oorspronkelijk bericht-----

Van: Commissie BiZa [redacted]
Verzonden: vrijdag 1 april 2011 14:40
Aan: Parlementaire Zaken BZK; Postbus minBZK
Onderwerp: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Origineel volgt per post.

Commissie BiZa

Aan de minister van
Binnenlandse Zaken en Koninkrijksrelaties
Mr. J.P.H. Donner

Plaats en datum: Den Haag, 1 april 2011
Betreft: Op afstand afluisteren van mobiele telefoons bij de overheid
Ons kenmerk: 32500-VII-91/2011D16997

Geachte heer Donner,

In de procedurevergadering van de vaste commissie voor Binnenlandse Zaken van 31 maart 2011 is gesproken over uw brief inzake het op afstand afluisteren van mobiele telefoons bij de overheid.
De commissie heeft besloten u te verzoeken de Kamer zo spoedig mogelijk te informeren over de resultaten van het onderzoek dat in gang is gezet, en over de maatregelen die reeds genomen zijn of waartoe de onderzoeksresultaten aanleiding geven.
De commissie ontvangt voorts graag een overzicht van de huidige maatregelen met betrekking tot de beveiliging van data bij de overheid (bijv. e-mailverkeer, data-opslag etc.).

Naar aanleiding van uw brief zijn in de commissie de volgende vraagpunten aan de orde gesteld.
- Monitoring van ICT-systemen binnen de overheid is van groot belang. Heeft de overheid zicht op wat er gebeurt op haar netwerken, waaronder mailsystemen, en kan ze tijdig ingrijpen als er sprake is van een onbewuste hiaat in de beveiliging of een doelbewuste inbreuk op de beveiliging ?
- Goed opdrachtgeverschap. In hoeverre vormt (informatie-)beveiliging een expliciet aandachtspunt bij een aanbesteding? Het grootste risico is dat in een aanbesteding beveiliging niet in de eisen wordt meegenomen. Bij wie is belegd dat (informatie)beveiliging standaard in aanbestedingen wordt meegenomen?
- Het wordt steeds gebruikelijker om eigen apparatuur te mogen gebruiken op het zakelijke netwerk ('bring your own device' beleid). Dit vergt een goede en veilige infrastructuur. Hoe is dit geregeld bij de overheid en hoe verhoudt dit beleid zich tot het initiatief van enkele ministers om eigen toestellen te gebruiken tegen het advies van de departementale ICT-afdeling in?
- Om succesvol het nieuwe werken te kunnen invoeren in een organisatie is goede en veilige infrastructuur nodig. Hoe is dit geregeld bij de overheid?
- Eigen verantwoordelijkheid. Gebruikers hebben een eigen verantwoordelijkheid bij het veilig gebruiken van communicatiemiddelen en ICT. Hoe wordt dit veilige gebruik binnen de overheid gestimuleerd?
- Het GovCERT en het NBV hebben een taak om de overheid te adviseren en waarschuwen als er mogelijke beveiligingsrisico's zijn. Hebben zij ook een signalerende rol naar de leverancier van producten en diensten, waarin zij dit risico signaleren?

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

Bij deze breng ik u het verzoek en de vragen van de commissie over.

Hoogachtend,

[redacted]

[redacted]

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.biza@tweedekamer.nl

384

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 april 2011 14:11
Aan: [redacted]
Onderwerp: RE: Hierbij Vodafone

Dan[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 22 april 2011 14:10
Aan: [redacted]
Onderwerp: Hierbij Vodafone

Het bericht kan nu met het volgende bijlagen of koppelingen worden verzonden:

Voorbereiding spoeddebat 29 maart 2011.doc
[redacted]kamer+pincode+24+maart.pdf

Opmerking: Sommige e-mailprogramma's staan ter beveiliging tegen virussen het verzenden of ontvangen van bepaalde bestandsbijlagen niet toe. Controleer de beveiligingsinstellingen voor uw e-mail als u wilt weten hoe bijlagen worden afgehandeld.

385

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 april 2011 15:02
Aan: [redacted]
Onderwerp: Vodafone voicemail
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste [redacted]

In het kader van het voicemail incident van Vodafone hee[redacted]u eerder een mail (zie bijlage) gestuurd met het verzoek nummers van de politieke en ambtelijke top te verzamelen in het kader van het onderzoek in hoeverre de staatsveiligheid in geding is geweest. Tegelijk is aan Vodafone gevraagd in aantallen aan te geven in hoeverre gebruik is gemaakt van het op afstand beluisteren van de voicemail binnen het kader van het OT2010 contract. Ter informatie hierbij de vragen:
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

Vodafone heeft onze vragen inmiddels beantwoord, [redacted] Die aantallen zijn naar verhouding zeer gering, maar geven uiteraard niet aan bij welke nummers dat is gebeurd. Om meer zekerheid te verkrijgen over het probleem is het nodig verder te focussen. Daartoe zijn twee zaken nodig: 3+4
1) het overzicht van de telefoonnummers da[redacted]n zijn mail heeft gevraagd, te verstrekken. Vodafone zal worden gevraagd bovenstaande vragen te beantwoorden uitsluitend m.b.t. deze nummers.
2) een, in de woorden van Vodafone, 'bevel' om dit te onderzoeken.

Een en ander is afgelopen CBIB vergadering aangekondigd. **Graag ontvang ik van jullie op korte termijn (uiterlijk vrijdag 29 april, maar liefst eerder) het overzicht van deze nummers.** In verband met privacy en veiligheidsissues kan dit overzicht aan mij in een versleuteld zip bestand worden gestuurd met een SMS aan mij met het wachtwoord ervan. Mijn mobiele nummer staat in de handtekening bij dit bericht. Het kan ook op papier (per post of ter hand) naar mij worden gestuurd. Bij versturen van de nummers ook graag jullie individuele bevel tot onderzoek in de vorm van de zin "Hierbij beveel ik <naam>, beveiligingsambtenaar van het ministerie van <...> tot het verrichten van nader getalsmatig onderzoek naar het op afstand beluisteren van de voicemail voor de volgende mobiele telefoonnummers, volgend op het eerdere onderzoek dat in opdracht van het ministerie van BZK is gedaan".

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag[redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
M [redacted]
[redacted]
http://www.minbzk.nl
.....

[redacted]

Van: [redacted]

Verzonden: maandag 28 maart 2011 10:43

Aan: [redacted]

CC: [redacted]

Onderwerp: Vodafone voicemail incidenten

Urgentie: Hoog

Geachte [redacted],

hierbij mail ik jullie ter informatie de brief, die minister Donner afgelopen vrijdag naar de Tweede kamer heeft gezonden over de voicemail incidenten bij Vodafone.

In het kader van het onderzoek om te bezien of en in hoeverre de staatsveiligheid in het geding is geweest, verzoek ik jullie alvast de telefoonnummers te verzamelen van de politieke en ambtelijke top bij jullie departement (en wellicht andere voor dit onderwerp relevante) ambtenaren. Deze zullen we nodig hebben om uit te vinden, hoe vaak op de bijbehorende mailboxen in de laatste weken is ingebeld (ofwel met 3333, ofwel van buiten het Vodafone netwerk).
Als jullie suggesties hebben voor dit onderzoek, neem even contact met me op.

Er is sprake van, dat deze week nog een spoeddebat in de TK volgt.

Met vriendelijke groet,

[redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

[redacted]

Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag

[redacted]

T [redacted]

[redacted]

http://www.rijksoverheid.nl

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten Generaal

DGOBR/DIR

Schedeldoekshaven 200
2511 EZ Den Haag

Postbus 20011
2500 EA Den Haag

www.rijksoverheid.nl

Contactpersoon
Frank Heijligers

T (070) 426 8581
frank.heijligers@minbzk.nl

Datum 24 maart 2011
Betreft Op afstand afluisteren van mobiele telefoons bij de overheid

In het televisieprogramma Een Vandaag van 23 maart 2011 was te zien hoe op afstand de voicemailberichten konden worden beluisterd van ministers, burgemeesters, kamerleden, topambtenaren en woordvoerders bij de Nederlandse overheid. Op 24 maart 2011 hebben diverse media, waaronder Nieuwsuur en opnieuw Een Vandaag hieraan aandacht besteed. Met deze brief wil ik de Tweede Kamer inlichten over de feiten rond dit ernstig te noemen fenomeen en de genomen maatregelen ter zake.

Een van de diensten die bij mobiele telefonie hoort, is de mogelijkheid om op afstand vanaf een willekeurige telefoon de voicemail van de eigen mobiele telefoon te beluisteren. Om misbruik te voorkomen is dit afluisteren beveiligd met een pincode. Bij Vodafone is deze pincode standaard ingesteld op 3333. De gebruiker kan deze pincode zelf met zijn mobiele telefoon wijzigen in een eigen pincode. Naar nu blijkt had het voicemailsysteem van Vodafone te maken met twee afzonderlijke problemen.

Vodafone had sinds 2007 voor grootzakelijke klanten de mogelijkheid afgeschermd om met deze standaard ingestelde pincode via een willekeurige andere telefoon voicemailberichten op afstand af te luisteren. Echter door een fout bij Vodafone is het sinds november 2010 mogelijk geworden om deze standaard pincode daarvoor wel te gebruiken en is het misbruik dat door Een Vandaag is aangetoond, mogelijk geworden. Vodafone was niet op de hoogte van deze fout totdat Een Vandaag dit publiekelijk maakte. Ook de overheid was van deze fout niet op de hoogte. Vodafone heeft deze fout inmiddels publiekelijk erkend, de verantwoordelijkheid ervoor volledig op zich genomen en ons hun excuses aangeboden. Het genoemde misbruik raakte overigens alle Vodafone abonnees en niet alleen een groot gedeelte van de overheid. De Ministeries van Defensie en voormalig Justitie hebben een andere dienstverlener voor mobiele telefonie en deze voicemailboxen zijn niet door het incident geraakt.

Nadat Een Vandaag melding had gemaakt van de mogelijkheid op genoemde wijze voicemailberichten af te luisteren, heeft Vodafone terstond de fout hersteld. Vodafone heeft ons gemeld dat ze als gevolg van dit incident hun beveiligings- en privacybeleid opnieuw tegen het licht houden.

Het tweede probleem was dat het voicemailsysteem van Vodafone kwetsbaar was voor hetgeen technici 'callerID spoofing' noemen. Dit is een andere, technische meer ingewikkelde methode dan Een Vandaag in het programma van 23 maart heeft getoond. Hierbij stuurt een kwaadwillende een ander afzendernummer mee dan het feitelijke nummer van zijn eigen telefoon. Voor de voicemailcentrale lijkt het dan alsof de gebruiker met de eigen mobiele telefoon toegang wenst tot het voicemailsysteem. Deze methode werkt alleen, indien de gebruiker van de mobiele telefoon niet heeft aangegeven dat er een pincode nodig is voor het beluisteren van de voicemail via de eigen mobiele telefoon. Nieuwsuur heeft op 24 maart aandacht besteed aan deze vorm van identiteitsfraude. Dit probleem is door GovCERT eerder onder de aandacht gebracht van de beveiligingsambtenaren en de (operationele) informatiebeveiligers van alle ministeries en hoge colleges van staat zodat deze op hun beurt gebruikers op de hoogte konden stellen van ter zake passende maatregelen. Helaas moet ik constateren dat dit niet in alle gevallen is gebeurd. Het kabinet heeft eerder al besloten meer centraal te sturen op de ICT-veiligheid door in het kader van uitvoeringsprogramma Compacte Rijksdienst bij het ministerie van Veiligheid en Justitie een ICT-beveiligingsorganisatie in te richten.

Ook Vodafone was eerder op de hoogte van dit probleem en heeft gisteren deze kwetsbaarheid in hun voicemailsysteem opgelost. Deze geconstateerde kwetsbaarheid is in strijd met het contract dat met Vodafone is afgesloten dat te allen tijde voorziet in externe veilige toegang tot de voicemail door middel van een pincode.

Als gevolg van dit incident laat ik voor zover nog mogelijk, onderzoeken of er misbruik is gemaakt van deze fout en, indien daartoe aanleiding bestaat, in hoeverre staatsveiligheid in het geding is geweest. Voorts laat ik onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal ik betrekken bij het inrichten van de ICT-beveiligingsorganisatie.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.P.H. Donner

387

[redacted]

Van: [redacted]
Verzonden: zondag 24 april 2011 13:02
Aan: [redacted]
Onderwerp: RE: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Mooie start. Graag bespreken in MT volgende week. Architectuur toevoegen.
Groet,
[redacted]

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 22 april 2011 10:50
Aan: [redacted]
Onderwerp: RE: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

De pdf is een brief die de cie BZK van de Kamer naar minister Donner stuurde nav het Vodafone-incident.

Op verzoek van dgOBR: kijken welke kansen hierin zitten voor nieuw beleid.
Als bijlage (word-doc) een indeling van de vragen en de mogelijke beantwoordingslijn en/of discussiepunten
Als slot een kort procesvoorstel.

[redacted], kun jij ook de feitelijke vragen nog aanvullen?

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: donderdag 21 april 2011 16:24
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: vrijdag 1 april 2011 16:11
Aan: [redacted]
Onderwerp: FW: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Bij deze.

Groet, [redacted]

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Parlementaire Zaken / Bestuurszaken
tel.nr. [redacted]
-----Oorspronkelijk bericht-----

Van: [redacted]
Verzonden: vrijdag 1 april 2011 14:40
Aan: [redacted]
Onderwerp: Brief aan minister over op afstand afluisteren van mobiele telefoons bij de overheid

Origineel volgt per post.

390

[redacted]

Van: [redacted]
Verzonden: woensdag 27 april 2011 9:01
Aan: [redacted]
Onderwerp: FW: Vodafone voicemail
Gevoeligheid: Vertrouwelijk

Voor jou!

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 27 april 2011 8:43
Aan: [redacted]
Onderwerp: RE: Vodafone voicemail
Gevoeligheid: Vertrouwelijk

[redacted] wij zitten nu nog bij KPN heeft het zin onze nummers door te geven, lijkt mij niet. Vlgs mij is alleen DGV ([redacted]) of een deel van zijn DG aangesloten bij Vodafone.

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 april 2011 15:02
Aan: [redacted]
Onderwerp: Vodafone voicemail
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste leden van het CBIB,

In het kader van het voicemail incident van Vodafone heeft [redacted] u eerder een mail (zie bijlage) gestuurd met het verzoek nummers van de politieke en ambtelijke top te verzamelen in het kader van het onderzoek in hoeverre de staatsveiligheid in geding is geweest. Tegelijk is aan Vodafone gevraagd in aantallen aan te geven in hoeverre gebruik is gemaakt van het op afstand beluisteren van de voicemail binnen het kader van het OT2010 contract. Ter informatie hierbij de vragen:
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
[redacted]anaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

Vodafone heeft onze vragen inmiddels beantwoord, [redacted] Die aantallen zijn naar verhouding zeer gering, maar geven uiteraard niet aan bij welke nummers dat is gebeurd. Om meer zekerheid te verkrijgen over het probleem is het nodig verder te focussen. Daartoe zijn twee zaken nodig:
1) het overzicht van de telefoonnummers dat [redacted] in zijn mail heeft gevraagd, te verstrekken. Vodafone zal worden gevraagd bovenstaande vragen te beantwoorden uitsluitend m.b.t. deze nummers.
2) een, in de woorden van Vodafone, 'bevel' om dit te onderzoeken.

Een en ander is afgelopen CBIB vergadering aangekondigd. **Graag ontvang ik van jullie op korte termijn (uiterlijk vrijdag 29 april, maar liefst eerder) het overzicht van deze nummers.** In verband met privacy en veiligheidsissues kan dit overzicht aan mij in een versleuteld zip bestand worden gestuurd met een SMS aan mij met het wachtwoord ervan. Mijn mobiele nummer staat in de handtekening bij dit bericht. Het kan ook op papier (per post of ter hand) naar mij worden gestuurd. Bij versturen van de nummers ook graag jullie individuele bevel tot onderzoek in de vorm van de zin "Hierbij beveel ik <naam>, beveiligingsambtenaar van het ministerie van <...> tot het verrichten van nader getalsmatig onderzoek naar het op afstand beluisteren van de voicemail voor de volgende mobiele telefoonnummers, volgend op het eerdere onderzoek dat in opdracht van het ministerie van BZK is gedaan".

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag [redacted]
Postbus 20011 | 2500 EA | Den Haag
T [redacted]

[redacted]
http://www.minbzk.nl

****

Bezoekt u binnenkort een locatie van de Rijksoverheid?

Dan dient u in het bezit te zijn van een geldige Rijkspas of een geldig identiteitsbewijs (paspoort,
nationale identiteitskaart, rijbewijs of vreemdelingendocument). Indien u bij controle geen geldig identiteitsbewijs kunt tonen, wordt de toegang geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.

****

****

391

[redacted]

Van: [redacted]
Verzonden: woensdag 27 april 2011 9:41
Aan: [redacted]
Onderwerp: RE: Vodafone voicemail
Gevoeligheid: Vertrouwelijk

Laat ik je nog weten [redacted]

[redacted]

Van [redacted]
Verzonden: woensdag 27 april 2011 9:35
Aan [redacted]
CC: [redacted]
Onderwerp: RE: Vodafone voicemail
Gevoeligheid: Vertrouwelijk

[redacted]

Helder.
Mocht je het van belang vinden om [redacted] mee nemen in het onderzoek dan is zijn nummer wel nodig.

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haag | [redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
T [redacted]
[redacted]
http://www.minbzk.nl
.....

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 27 april 2011 9:01
Aan: [redacted]
Onderwerp: FW: Vodafone voicemail
Gevoeligheid: Vertrouwelijk

Voor jou!

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: woensdag 27 april 2011 8:43
Aan: [redacted]
Onderwerp: RE: Vodafone voicemail
Gevoeligheid: Vertrouwelijk

[redacted] wij zitten nu nog bij KPN heeft het zin onze nummers door te geven, lijkt mij niet. Vigs mij is alleen DGV[redacted]) of een deel van zijn DG aangesloten bij Vodafone.

[redacted]

Van: [redacted]
Verzonden: vrijdag 22 april 2011 15:02
Aan: [redacted]
Onderwerp: Vodafone voicemail
Urgentie: Hoog
Gevoeligheid: Vertrouwelijk

Beste [redacted]

In het kader van het voicemail incident van Vodafone heeft [redacted] u eerder een mail (zie bijlage) gestuurd met het verzoek nummers van de politieke en ambtelijke top te verzamelen in het kader van het onderzoek in hoeverre de staatsveiligheid in geding is geweest. Tegelijk is aan Vodafone gevraagd in aantallen aan te geven in hoeverre gebruik is gemaakt van het op afstand beluisteren van de voicemail binnen het kader van het OT2010 contract. Ter informatie hierbij de vragen:
a. hoe vaak is bij de abonnees onder het OT 2010 contract in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
b. bij hoeveel telefoonnummers onder het OT 2010 contract is in de betreffende periode gebruik gemaakt van de standaardpincode 3333 voor het afluisteren van voicemailboxen? Graag gespecificeerd naar periode (per week).
c. Vanaf hoeveel verschillende nummers zijn OT 2010 nummers met de standaardpincode 3333 gebeld voor het afluisteren van de voicemailbox en wat is het aantal acties per nummer? Graag specificeren naar aantal nummers binnen het OT2010 contract, binnen Nederland, buiten Nederland.

Vodafone heeft onze vragen inmiddels beantwoord [redacted] Die aantallen zijn naar verhouding zeer gering, maar geven uiteraard niet aan bij welke nummers dat is gebeurd. Om meer zekerheid te verkrijgen over het probleem is het nodig verder te focussen. Daartoe zijn twee zaken nodig:
1) het overzicht van de telefoonnummers da[redacted]n zijn mail heeft gevraagd, te verstrekken. Vodafone zal worden gevraagd bovenstaande vragen te beantwoorden uitsluitend m.b.t. deze nummers.
2) een, in de woorden van Vodafone, 'bevel' om dit te onderzoeken.

Een en ander is afgelopen CBIB vergadering aangekondigd. Graag ontvang ik van jullie op korte termijn (uiterlijk vrijdag 29 april, maar liefst eerder) het overzicht van deze nummers. In verband met privacy en veiligheidsissues kan dit overzicht aan mij in een versleuteld zip bestand worden gestuurd met een SMS aan mij met het wachtwoord ervan. Mijn mobiele nummer staat in de handtekening bij dit bericht. Het kan ook op papier (per post of ter hand) naar mij worden gestuurd. Bij versturen van de nummers ook graag jullie individuele bevel tot onderzoek in de vorm van de zin "Hierbij beveel ik <naam>, beveiligingsambtenaar van het ministerie van <...> tot het verrichten van nader getalsmatig onderzoek naar het op afstand beluisteren van de voicemail voor de volgende mobiele telefoonnummers, volgend op het eerdere onderzoek dat in opdracht van het ministerie van BZK is gedaan".

Met vriendelijke groet,

[redacted]
senior beleidsmedewerker

.....
Ministerie van BZK
Directoraat Generaal Organisatie en Bedrijfsvoering Rijk
[redacted]
Schedeldoekshaven 200 | 2511 EZ | Den Haa[redacted]
Postbus 20011 | 2500 EA | Den Haag
.....
[redacted]
http://www.minbzk.nl
.....

****
Bezoekt u binnenkort een locatie van de Rijksoverheid?

Dan dient u in het bezit te zijn van een geldige Rijkspas of een geldig identiteitsbewijs (paspoort,
nationale identiteitskaart, rijbewijs of vreemdelingendocument). Indien u bij controle
geen geldig identiteitsbewijs kunt tonen, wordt de toegang geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.

****
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de
geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u
verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat
aanvaardt geen aansprakelijkheid voor schade, van welke aard dan ook, die verband
houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not
the addressee or if this message was sent to you by mistake, you are requested to
inform the sender and delete the message. The State accepts no liability for

damage of any kind resulting from the risk inherent in the electronic transmission
of messages.
****