Communicatie met GOVCERT

From: ,GOVCERT.NL) govcert.nl>
Sent: vrijdag 25 maart 2011 09:42
To:
Subject: Status Vodafone

Ik heb nog even geschakeld met de mensen die zich binnen GOVCERT.NL bezighouden met de Vodafone-case en het blijkt dat er vanochtend nog de nodige communicatie wordt rondgestuurd aan alle deelnemers over dit issue. Ik heb gevraagd hier ook de zaken in op te nemen die we vanochtend aan de telefoon bespraken. Het lijkt me handig om deze communicatie als bevestiging en leidend te gebruiken.

Met vriendelijke groet,

Security Specialist

GOVCERT.NL
T
I www.govcert.nl
E @govcert.nl

PGP Fingerprint: 5A2E 93EC 60C6 99F3 B833 DBC0 544D 12A5 79FC 6732

P.O. Box 84011
2508 AA The Hague
The Netherlands

GOVCERT.NL is the Cyber Security & Incident Resporse Team for the Dutch Government. We support the government and organisations with a public task in preventing and dealing with IT-related security incidents.

From:
Sent: vrijdag 25 maart 2011 12:08
To: @govcert.nl
Subject: RE: Status Vodafone

Beste

Dank.
Groet,

-----Original Message-----
From: (GOVCERT.NL) [mailto govcert.nl]
Sent: vrijdag 25 maart 2011 9:42
To:
Subject: Status Vodafone

Ik heb nog even geschakeld met de mensen die zich binnen GOVCERT.NL bezighouden met de Vodafone-case en het blijkt dat er vanochtend nog de nodige communicatie wordt rondgestuurd aan alle deelnemers over dit issue. Ik heb gevraagd hier ook de zaken in op te nemen die we vanochtend aan de telefoon bespraken. Het lijkt me handig om deze communicatie als bevestiging en leidend te gebruiken.

Met vriendelijke groet,

Security Specialist

GOVCERT.NL
T
I www.govcert.nl
E govcert.nl

PGP Fingerprint: 5A2E 93EC 60C6 99F3 B833 DBC0 544D 12A5 79FC 6732

P.O. Box 84011
2508 AA The Hague
The Netherlands

GOVCERT.NL is the Cyber Security & Incident Response Team for the Dutch Government. We support the government and organisations with a public task in preventing and dealing with IT-related security incidents.

From:
Sent: vrijdag 25 maart 2011 11:01
To:
Subject: Fw: Factsheet: kwetsbaarheden in voicemaildiensten
Attachments: FS-2011-02 Kwetsbaarheden in voicemaildiensten 1.1.pdf

NB!

----- Oorspronkelijk bericht -----
Van: [mailto: @govcert.nl]
Verzonden: Friday, March 25 2011 10:53 AM
Aan: @lists.govcert.nl @lists.govcert.nl>, @lists.govcert.nl @lists.govcert.nl> @govcert.nl @govcert.nl>
Cc: @minaz.nl @minaz.nl>; @minbzk.nl @minbzk.nl>; @mindef.nl < @mindef.nl>; @minez.nl @minez.nl>; @minfin.nl @minfin.nl> @minjus.nl @minjus.nl>; @minlnv.nl @minlnv.nl>; @minocw.nl @minocw.nl> @minszw.nl @minszw.nl>; @minvenw.nl @minvenw.nl>; @minvenw.nl @minvenw.nl>; @minvws.nl @minvws.nl>; @minvrom.nl @minvrom.nl>; @tweedekamer.nl @tweedekamer.nl>
Onderwerp: Factsheet: kwetsbaarheden in voicemaildiensten

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Beste

De problematiek rondom de voicemaildienst van Vodafone behoeft geen introductie.

Naar aanleiding van de ontwikkelingen van de afgelopen dagen hebben we de
feiten in een factsheet verwerkt.

In de factsheet kunt u kort nog over de inmiddels opgeloste kwetsbaarheden
lezen. Ons advies van 21 januari, het instellen van een pincode, blijft overigens van kracht. Ook dat kunt u in de factsheet lezen.

Met vriendelijke groet,

GOVCERT.NL
T
I www.govcert.nl
E govcert.nl
PGP Fingerprint: 5EF4 6F80 7530 1583 E140 D918 BC24 36AC 1045 1333

GOVCERT.NL is the Cyber Security & Incident Response Team for the Dutch Government. We support the government and organisations with a public task
in preventing and dealing with IT-related security incidents.

-----BEGIN PGP SIGNATURE-----
Version: PGP Desktop 10.1.1 (Build 10)
Charset: utf-8

wj8DBQFNjGXTvCQ2rBBFEzMRAsOIAJ9O60RxZJ7WygXPgsZuHRHvXI2uOACfUvJM
xmVdU20WpyZSTuw6xKcupl0=
=27wn
-----END PGP SIGNATURE-----

GOVCERT.NL

Factsheet FS-2011-02
Kwetsbaarheden in voicemaildiensten

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.

Op 21 januari 2011 heeft GOVCERT.NL haar deelnemers gewaarschuwd voor de kwetsbaarheid die op 24 maart bekend is geworden. In deze factsheet leggen wij beknopt de aard van de kwetsbaarheden uit.

Daarnaast herhalen wij het advies dat wij destijds aan onze deelnemers gaven. Dit advies blijft, hoewel deze specifieke kwetsbaarheden inmiddels zijn opgelost, van kracht.

De feiten op een rij:

> Er zijn twee kwetsbaarheden bekend gemaakt in de voicemaildienst van Vodafone.

> GOVCERT.NL heeft geverifieerd dat beide kwetsbaarheden inmiddels verholpen zijn door Vodafone.

> Deze factsheet is ook relevant voor klanten van andere telecomproviders.

> Ons advies blijft:

- Gebruik *nooit* een 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.

Om welke kwetsbaarheden ging het?

De informatie betrof twee kwetsbaarheden:

1. Een kwetsbaarheid als gevolg van onjuist gebruik van een standaard pincode.
2. Een kwetsbaarheid als gevolg van authenticatie, uitsluitend op basis van *caller-ID* (het nummer waarmee gebeld wordt).

GOVCERT.NL heeft op 24 en 25 maart diverse tests uitgevoerd en kan bevestigen dat beide kwetsbaarheden zijn verholpen. Op basis daarvan schatten wij in dat Vodafone aan het begin van de avond van 24 maart is begonnen met het stapsgewijs uitrollen van een fix, en dat de fix in de loop van de nacht volledig uitgerold was.

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 pincode niet van de standaard pincode (bij Vodafone 3333) 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 men elk willekeurig caller-ID kan gebruiken. 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 konden de gevolgen van deze kwetsbaarheden zijn?

Beide kwetsbaarheden die hierboven zijn beschreven konden worden gebruikt om de voicemail van een ander af te luisteren. Met andere woorden: derden konden zich toegang verschaffen tot uw voicemail en binnengekomen berichten beluisteren.

From:
Sent: vrijdag 8 april 2011 16:48
To:
Subject: Fw: Factsheet 'Veilig gebruik van smartphones en tablets'
Attachments: Factsheet FS 2011-03 Smartphones v1 0.pdf

Van: (GOVCERT.NL) [mailto: @govcert.nl]
Verzonden: Friday, April 08, 2011 03:48 PM
Aan: @minbzk.nl>; minaz.nl @minaz.nl>; @minfin.nl>; minder.nl>; minbzk.nl minbzk.nl>; @minbzk.nl @minbzk.nl>; minjus.nl>; @minbzk.nl>; @minvws.nl minvws.nl>; @minbzk.nl>; @minlnv.nl @minlnv.nl>; @minocw.nl @minocw.nl>; MINSZW.NL @MINSZW.NL>; @minbzk.nl minbzk.nl>; minez.nl @minez.nl>; @tweedekamer.nl @tweedekamer.nl>; @minjus.nl>; @minbzk.nl>; @minvenw.nl @minvenw.nl>; @minbzk.nl>; @mindef.nl @mindef.nl>; @minaz.nl>; kabinetderkoningin.nl @kabinetderkoningin.nl>
Onderwerp: Factsheet 'Veilig gebruik van smartphones en tablets'

Collega's,

Bijgevoegd vindt u zoals eerder aangekondigd de factsheet "Veilig gebruik van smartphones en tablets", die we vandaag publiceren.

Deze factsheet bevat een beknopt overzicht van de risico's en de belangrijkste maatregelen die een gebruiker kan nemen om het risico van dataverlies te verkleinen. Deze factsheet stellen wij ook publiek beschikbaar via onze website.

Mocht u de sheet met tips die ik vorige week stuurde geschikter vinden voor bepaalde doelgroepen in uw organisatie, gebruikt u die dan gerust in aanvulling op deze factsheet. De betreffende sheet maken wij niet publiek en blijft bedoeld voor gebruik binnen alleen de rijksoverheid.

Indien u vragen, op- of aanmerkingen heeft over de factsheet, dan horen we dat graag.

Vriendelijke groet,

From: (GOVCERT.NL)
Sent: vrijdag 1 april 2011 14:44
To: @minaz.nl; ; @minbzk.nl; minbzk.nl; @minvws.nl; F @minlnv.nl; @minocw.nl; @MINSZW.NL; @minbzk.nl; @minez.nl; tweedekamer.nl: @minvenw.nl; mindef.nl; @kabinetderkoningin.nl
Subject: RE: Betr: RE: Veilig bellen in vandaag (en in CBIB van 13 april?)

Collega's.

Zoals ik gisteren in ons overleg heb toegezegd, stuur ik u bijgevoegd de digitale versie van de 'Tips voor veilig gebruik van mobiele telefoons'. Dit document is gisteren ook op papier beschikbaar gesteld.

Let wel: dit is nog niet onze officiële factsheet over smartphones, maar een afgeleide daarvan. De officiële factsheet over dat onderwerp publiceren we zsm. Daarom het verzoek de bijlage vooral te benutten om opvolging te kunnen geven aan de vragen die zijn gerezen in de van vorige week.

Alvast een fijn weekend gewenst.

Vriendelijke groet,

Teamleider Kenniscentrum
GOVCERT.NL

T 070
M 06

Postbus 84011, 2508 AA Den Haag

Out of Scope

GOVCERT.NL

Factsheet FS 2011-03

Veilig gebruik van smartphones en tablets

Naast bellen en sms'en kun je met een smartphone goed internetten, e-mailen en applicaties (zogenaamde apps) downloaden en gebruiken. Het merendeel van de Nederlanders (64%) gaat niet de deur uit zonder smartphone, bijna een derde gaat er zelfs mee naar bed[1]. Door de alsmaar toenemende capaciteit en functionaliteit, evenals de toenemende netwerkcapaciteit van mobiel internet, worden smartphones steeds vaker met bedrijfsnetwerken geïntegreerd.

In deze factsheet leest u wat de belangrijkste beveiligingsrisico's zijn aan het gebruik van een smartphone, tablet of mobiel besturingssysteem en hoe u zowel zakelijk als privé op een verstandige manier met deze beveiligingsrisico's om kunt gaan en mogelijke schade kan voorkomen of beperken.

De belangrijkste feiten op een rij:

- > De grens tussen privé- en zakelijk gebruik van de smartphone vervaagt
- > Het aanbod en aantal downloads van apps voor de smartphone groeit enorm.
- > Het 'op straat' komen liggen van vertrouwelijke informatie is het grootste beveiligingsrisico.
- > De dreiging van malware-aanvallen op smartphones is nog klein, maar groeit.
- > Via een aantal kleine handelingen is de beveiliging van de smartphone te vergroten.

De veelgebruikte apps op smartphones verwerken of wisselen in meer of mindere mate vertrouwelijke of gevoelige informatie uit. De smartphone is de mobiele *front-end* van centraal opgeslagen informatie. Denk hierbij aan uw contacten, e-mails, agenda afspraken en documenten. Dit brengt beveiligingsrisico's met zich mee.

Risico's van integratie smartphones met bedrijfsnetwerken

Uit onderzoek van Juniper Networks[2] blijkt dat veel werknemers, via hun smartphone, bedrijfsnetwerken van hun werkgevers zonder toestemming benaderen. Deze ongeautoriseerde smartphones zijn een gevaar voor de bedrijfsveiligheid. Denk hierbij aan het lekken van (bedrijfs)informatie door apps op de smartphone en het afluisteren van bijvoorbeeld Bluetooth en Wifi. Het 'op straat' komen liggen van vertrouwelijke of gevoelige informatie is het grootste beveiligingsrisico.

U als werknemer dient zich natuurlijk te allen tijde aan het informatiebeveiligingsbeleid en -richtlijnen van uw werkgever te conformeren. Het advies is dan ook om tijdens uw werkzaamheden alleen gebruik te maken van de door uw werkgever verstrekte smartphone of toestemming te vragen aan uw werkgever voor gebruik van uw privé smartphone. Als de smartphone door de werkgever is verstrekt dan zijn daarop mogelijk al diverse beveiligingsmaatregelen ingesteld.

Tips om veilig gebruik te maken van smartphones

De drie belangrijkste beveiligingsmogelijkheden van de smartphone zijn: authenticatie van de gebruiker; versleuteling van de opgeslagen gegevens en het op commando wissen van de opgeslagen gegevens (eventueel op afstand).

Uw smartphone kwijt of gestolen?

Neem maatregelen zodat bij verlies of diefstal geen (vertrouwelijke of gevoelige) informatie op straat komt te liggen:

- Beveilig de toegang tot uw smartphone door middel van een toegangscode die door derden niet makkelijk te raden is[3]. Selecteer altijd de methode die de sterkste beveiliging biedt en wijzig

[1] http://www.synovate.nl/nieuws/20090908001/news.aspx, d.d. 8 september 2009
[2] http://www.juniper.net/us/en/company/press-center/press-releases/2010/pr_2010_10_26-10_02.html
[3] http://www.waarschuwingsdienst.nl/Computer+beveiligen/Wachtwoorden/Moeilijke+wachtwoorden+op+een+makkelijke+manier.html

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 93810
2509 JE Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

regelmatig uw toegangscode. De SIM-kaart heeft een eigen toegangscode en wij adviseren om deze toegangscode ook regelmatig te wijzigen.
Let op: Op het moment dat een kwaadwillende de verwijderbare media uit uw smartphone heeft verwijderd, heeft deze toegang tot alle 'onbeveiligde' gegevens die hierop zijn opgeslagen. De toegangscode beveiligt alleen de smartphone en niet de losse verwijderbare media zoals de (micro-)SD-kaart. Het advies is dan ook om naast deze maatregel alle informatie[4] op de smartphone te versleutelen.

- Stel uw smartphone zo in dat na een ingestelde tijdsperiode (bijv. 1 minuut) de smartphone automatisch wordt vergrendeld. Deze maatregel is effectief in combinatie met een toegangscode.
- Activeer de functionaliteit waarmee informatie[5] op uw smartphone standaard versleuteld opgeslagen wordt. De informatiebeveiligingsfunctionaris van uw organisatie kan u hierbij adviseren.
- Stel uw smartphone zo in dat na een aantal mislukte inlogpogingen (bijv. 10) de smartphone wordt gereset naar de standaard fabrieksinstellingen en uw informatie op de smartphone wordt gewist. Het advies is om naast deze maatregel regelmatig een reservekopie te maken van de gegevens op uw smartphone.
- Maak gebruik van een toepassing die het beheren van uw smartphone op afstand ondersteunt[5], zodat u bij vermissing controle houdt over uw smartphone, zie het kader "Functionaliteit op afstand".
  Let op: Deze functionaliteit werkt niet op het moment dat de smartphone uit staat, in vliegtuigmodus staat of de SIM-kaart is verwijderd of verwisseld.
  Beveiligingstoepassingen van derden[6] bieden de functionaliteit om een SMS te versturen als de SIM-kaart in uw smartphone wordt verwisseld door een andere SIM-kaart. Op deze manier kunt u uw smartphone toch lokaliseren en wissen.
- Maak regelmatig een reservekopie/back-up van uw smartphone zodat u bij vermissing of het defect raken van uw smartphone niet uw informatie kwijt bent. Voor het maken van een reservekopie/back-up hebt u een beheertoepassing nodig die is geïnstalleerd op uw computer[7].
- Bewaar de International Mobile Equipment Identity (IMEI)-code[8] op een veilige plek en gescheiden van uw smartphone. De IMEI-code is een 15-cijferig nummer en is de unieke identificatie (serienummer) van uw smartphone. Deze IMEI-code heeft u nodig om bij verlies of diefstal aangifte te doen bij de politie.
- Doe altijd aangifte bij de politie als u merkt dat uw smartphone is verdwenen. Wanneer u uw smartphone gebruikt voor werk, meldt het dan ook bij de hiervoor aangewezen instantie binnen uw organisatie (bijvoorbeeld beveiliging of facilitaire zaken). Daarnaast kunt u het ook registreren in het 'telefooncheck' register[9].

Functionaliteit op afstand

Er zijn programma's voor smartphones die functionaliteit bieden die op afstand kan worden uitgevoerd, bijvoorbeeld in het geval dat u uw telefoon bent verloren. Hieronder enkele voorbeelden van dergelijke functionaliteit.

> Het wissen van informatie en het resetten naar de standaard fabrieksinstellingen.

> Het lokaliseren van uw smartphone zodat u op een kaart ziet waar uw smartphone zich bevindt;

> Een bericht op het display weergeven zodat de vinder weet waar de smartphone kan worden terugbezorgd;

> Een nieuwe toegangscode instellen om uw smartphone te beveiligen.

Lever uw smartphone 'schoon' in.

Op het moment dat u uw smartphone verkoopt of weggeeft aan iemand anders adviseren wij de fabrieksinstellingen te herstellen en alle informatie te wissen. Denk hierbij aan uw contactgegevens, sms'jes, e-mails, de door u geïnstalleerde apps en instellingen. Het wissen voorkomt dat de nieuwe eigenaar toegang heeft tot de achtergebleven informatie op de smartphone.

[4] Denk hierbij aan het interne werkgeheugen, interne opslag en verwijderbare opslagmedia.
[5] Voorbeelden hiervan zijn: iPhone: MobileMe <www.me.com/>; Windows Mobile: Micorsoft's My Phone <www.myphone.microsoft.com>; Android: Mobile Defense app <www.mobiledefense.com/> ; BlackBerry: SmrtGuard < www.smrtguard.com/>, BuddyGuard Pro <appworld.blackberry.com/webstore/content/10813?lang=en>
[6] http://www.av-comparatives.org/images/stories/test/mobile/mobile2010_english.pdf en http://mobile-security-software-review.toptenreviews.com/
[7] Voobeelden: Apple's iTunes en BlackBerry Desktop Software
[8] U vindt het IMEI-nummer door op u mobiele telefoon *#06# in te toetsen.
[9] http://www.telefooncheck.nu/index.php

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

Voorkom een virusinfectie op uw smartphone.

Een van de trends uit het 'Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010[10]' is dat de dreiging van malware-aanvallen[11] op smartphones nog klein is, maar groeit.
Criminelen maken misbruik van kwetsbaarheden van uw smartphone of u downloadt een 'onschuldig' lijkende app, die zonder dat u dat door heeft geheime, kwaadaardige functies (het trojaanse paard). bevat.

Als uw smartphone is geïnfecteerd met kwaadaardige software (malware) kunnen criminelen bijvoorbeeld:

- Zien wat u intypt om zo gebruikersnamen, wachtwoorden of andere (vertrouwelijke) informatie te achterhalen[12].
- Informatie verzamelen en verzenden naar een centrale server[13].
- SMS'jes versturen naar (dure) servicenummers of een abonnement afsluiten[14] zonder dat u daarvan op de hoogte bent.

Wij adviseren u om terughoudend te zijn met het installeren van onbekende apps op uw smartphone. Controleer vooraf de betrouwbaarheid van zowel de app als de makers. Bronnen die hierbij geraadpleegd kunnen worden zijn reviews van de app in de 'app store', of de ICT-afdeling van uw organisatie. Installeer alleen apps op het moment dat het initiatief voor de app bij u ligt of deze wordt gedistribueerd via de ICT-afdeling van uw organisatie. Ga bewust om met beveiligingsinstellingen van de apps, controleer altijd of deze in lijn zijn met de richtlijnen van uw organisatie. Geef alleen toestemming (rechten) aan apps op het moment dat u zeker bent van de impact en risico's. Voorzie uw smartphone, incl. apps, altijd van de laatste beveiligingsupdates / software versies.

Laat uw smartphone niet afluisteren.

Smartphones beschikken over een breed scala aan draadloze netwerken zoals WiFi en Bluetooth. Deze draadloze netwerken zijn in meer of mindere mate kwetsbaar voor afluisteren, waardoor informatie kan worden onderschept. Daarnaast kan gevoelige informatie langs andere weg uitlekken, bijvoorbeeld door zwakheden in de beveiliging van gsm-communicatie kunnen telefoongesprekken en sms-berichten worden afgeluisterd en ook is gebleken dat voicemails door derden af te luisteren kunnen zijn.

Wij adviseren u om de volgende maatregelen in acht te nemen:

- Schakel WiFi en Bluetooth uit wanneer u daar geen gebruik van maakt,
- Wees bewust en kritisch waar en wanneer u van een publiek (niet versleuteld) WiFi-netwerk gebruik maakt. Het is af te raden om op openbare plaatsen van een publiek WiFi-netwerk gebruik te maken. Als u dat toch doet, vermijd dan werk of financiële activiteiten. Stel daarnaast uw smartphone zo in dat het niet automatisch verbinding maakt met een WiFi-netwerk.
- Lees het factsheet "Afluisteren van GSM-communicatie"[15] aandachtig door. Het beschrijft de beveiliging van gsm en sms, de kwetsbaarheden die in de beveiliging zitten, de hierdoor veranderende risico's en hoe u zich hiertegen kunt beschermen.
- Lees het factsheet "Kwetsbaarheden in voicemaildiensten"[16] aandachtig door. Het beschrijft kwetsbaarheden in voicemaildiensten en hoe u zich hiertegen kunt beschermen.

Geef geen informatie via uw smartphone vrij.

Uit diverse onderzoeken blijkt dat een deel van de apps voor smartphones data van individuele gebruikers (bijvoorbeeld persoons- en locatiegegevens) verzamelen en deze op de achtergrond doorsturen naar derden (bijv. externe servers, ontwikkelaars of adverteerders), zonder de gebruiker te informeren[17]. In veel gevallen gaat het om de volgende gegevens: toestel-id, telefoonnummers en

[10] http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html
[11] Zie 'http://www.waarschuwingsdienst.nl/Begrippenlijst#M' voor een definitie van malware.
[12] Bijvoorbeeld het Zeus botnet. http://www.portablegear.nl/nieuws/11567/Zeus_botnet_bedreigt_smartphones.htm
[13] Bijvoorbeeld het mobiel botnet. http://www.automatiseringgids.nl/technologie/telecom/2010/52/eerste-mobiel-botnet-gesignaleerd.aspx
[14] Bijvoorbeeld het SMS-trojan. http://www.portablegear.nl/nieuws/11085/Eerste_SMS-trojan_voor_Android-smartphones_gedetecteerd.htm
[15] http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-gsm-communicatie.html
[16] http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemaildiensten.html
[17] http://www.nu.nl/internet/2302240/veel-gratis-applicaties-sturen-gevoelige-data-door.html, http://webwereld.nl/nieuws/67335/meeste-android-apps-lekken-priv--gegevens.html en http://webwereld.nl/nieuws/67365/meerderheid-iphone-apps-lekt-priv--gegevens.html.

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl

contactpersonenlijst. Apps worden door u geïnstalleerd, vaak zonder dat u weet wie de ontwikkelaar is en wat de programmacode is. Hierbij geeft u soms toestemming voor toegang tot informatie op uw telefoon zonder te weten wat hiermee wordt gedaan.

Ook hebben steeds meer apps de mogelijkheid om locatiegegevens toe te voegen aan tweets, foto's, video's of welk ander digitaal bestand (*geotagging*). Uw 'volgers' kunnen zo precies zien waar u was op het moment van het maken van een foto of het plaatsen van een bericht. Dit is natuurlijk ook de doelstelling van de op locatie gebaseerde diensten. Uit onderzoek blijkt dat privacy, meer transparantie en controle over hoe en met wie de locatiegegevens worden gedeeld zorgpunten zijn bij de gebruikers van deze functionaliteit[18].

Om onbewust vrijgeven van informatie te voorkomen of dit zoveel mogelijk te beperken adviseren wij u het volgende:

- Lees het factsheet "Veilig op sociale netwerken"[19] aandachtig door. Hierin wordt een overzicht gegeven van de beveiliging- en privacyrisico's verbonden aan deelname aan sociale netwerken. Daarnaast wordt een drietal veel voorkomende aanvalsmethoden, evenals enkele maatregelen voor veilig(er) gebruik van sociale netwerken beschreven.
- Kijk kritisch naar de standaard instellingen van uw toestel ten aanzien van beveiliging, privacy en connectiviteit. Beperk het delen van of de toegang tot informatie (zoals locatiegegevens) wanneer dit niet nodig is.
- Lees voordat u een app installeert de voorwaarden en privacybeleid door van de aanbieder, zodat u op de hoogte bent hoe er met uw gegevens wordt omgegaan. Als er geen voorwaarden of privacybeleid bestaat probeer dan op een andere manier deze informatie boven water te krijgen. Bronnen die hierbij geraadpleegd kunnen worden zijn reviews van de app of aanbieder in de 'app store', onafhankelijke testrapporten van de app of de ICT-afdeling van uw organisatie.

Wees voorzichtig bij online opslag.

Er zijn veel leveranciers die online opslag van foto's, documenten of back-ups aanbieden. Deze online opslag vindt meestal in de 'cloud'[20] plaats. De beveiliging van dergelijke diensten heeft u niet zelf in de hand en is niet altijd afdoende, wees dus voorzichtig bij online opslag vanaf uw smartphone. U moet altijd voorzichtig zijn met het online opslaan van uw vertrouwelijke gegevens. De online bestanden zijn direct toegankelijk voor iedereen die uw inloggegevens (vaak gebaseerd op e-mailadres en wachtwoord) weet te achterhalen.

Om op een veilige manier gebruik te maken van online opslag adviseren wij u het volgende:

- Maak bij het synchroniseren van u gegevens met de online opslag gebruik van een versleutelde verbinding. Informeer bij de dienstverlener van de online opslag of dit wordt ondersteund.
- Schrijf uw inloggegevens niet op. Als u dat toch doet bewaar uw inloggegevens dan op een veilige plek en gescheiden van uw smartphone.
- Versleutel uw bestanden voordat deze online worden geplaatst.
- Wijzig regelmatig uw wachtwoord.

Zie ook het whitepaper "Beveiliging van mobiele apparatuur en datadragers"[21] voor meer beveiligingstips.

Overige tips:

> Informeer binnen uw organisatie of er beleid, richtlijnen en/of standaarden zijn met betrekking tot het gebruik van smartphones.

> Schaf nieuwe apps voor uw smartphone altijd aan via officiële distributiekanalen van leveranciers, de zogenaamde 'app stores'.

> Wees u bewust dat u extra risico loopt als u uw smartphone 'Jailbreakt', omdat uw smartphone niet meer wordt beschermd door de beveiligingsmaatregelen die de leverancier heeft ingebouwd.

> Installeer indien mogelijk een virusscanner[6] op uw smartphone.

[18] http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/01/26/location-and-privacy-where-are-we-headed-on-data-privacy-day-natural-user-interface.aspx
[19] http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-het-gebruik-van-sociale-netwerken-voor-werknemers.html
[20] Zie 'http://nl.wikipedia.org/wiki/Cloud_computing' voor een definitie van de 'cloud'.
[21] http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/beveiliging-van-mobiele-apparatuur-en-datadragers.html