

Ven-1

From: [REDACTED]@fox-it.com]
Sent: vrijdag 14 januari 2011 13:07
To: [REDACTED] (GOVCERT.NL); [REDACTED]@minbzk.nl
Subject: FW: Fox Informatiebeveiliging: Voicemail
Signed By: There are problems with the signature. Click the signature button for details.

Importance: High

Misschien interessant om intern iets mee te doen.

Het zou ook zo maar prima voor andere providers kunnen werken. Dat moet nog even getest worden. Hier heeft iedereen nu een account bij spoofcard.com en zit elkaars voicemail uit te luisteren.

From [REDACTED]
Sent: vrijdag 14 januari 2011 13:04
To: All
Subject: Fox Informatiebeveiliging: Voicemail
Importance: High

FOX INFORMATIEBEVEILIGING



Voicemail

Beste collega's,

Met de overgang naar Vodafone is ook je voicemail onlangs gewijzigd. Het blijkt redelijk eenvoudig te zijn om toegang te krijgen tot de berichten van andermans voicemail. Als jouw voicemail-berichten regelmatig vertrouwelijk van aard zijn, dan is het aan te bevelen je voicemail zo in te stellen dat **altijd** om een PIN-code wordt gevraagd. Standaard vraagt je voicemail alleen om een PIN-code als je belt van je eigen toestel, maar dit blijkt eenvoudig te omzeilen.

Om altijd naar je PIN-code te laten vragen, bel je met **1233**. In het menu kies je vervolgens 2, 5, 3 en 1.

Hebben jullie vragen of opmerkingen, dan hoor ik deze graag.

Groet,

[REDACTED]
Beveiligingsfunctionaris

PS: Meer informatie over beveiliging bij Fox vind je op Foxwiki:
<https://foxwiki/foswiki/bin/view/FoxIt/FoxInformatieBeveiliging>

Venj-2-Vodafone voicemail eenvoudig af te luisteren
From: [REDACTED] (GOVCERT.NL)
Sent: dinsdag 18 januari 2011 10:57
To: [REDACTED] (GOVCERT.NL)
Subject: Vodafone voicemail eenvoudig af te luisteren

Beste DSC-ers, IB-ers en Beveiligingsambtenaren,

Uit de testen blijkt dat het eenvoudig is om de voicemail boxen van willekeurige Vodafone gebruikers af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatie mechanisme gebruikt voor het beluisteren van de voicemail-box. Standaard wordt hierbij niet om een PIN code gevraagd. Het caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

Naar aanleiding van een Blog-post van 30-05-2010
(<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-for-authentication/>)
heeft het beveiligingsbedrijf Fox-IT een aantal testen uitgevoerd op de beveiliging van voicemail op het Vodafone netwerk wat het bovenstaande bevestigt.

Wij adviseren u na te gaan wie er binnen uw organisatie gebruik maakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. (Standaard staat hier geen PIN-code op).

Met vriendelijke groeten,
GOVCERT.NL

--

[REDACTED]
security specialist

GOVCERT.NL
T +31 70 888 75 55
I www.govcert.nl
[REDACTED]@govcert.nl

PGP Fingerprint: C87E 47E2 89D8 5DFB C86F A3F3 1557 E2E9 AC15 7DD5

GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government. We support the government in preventing and dealing with IT-related security incidents.

VenJ-3-Vodafone caller-ID spoofing
From: [REDACTED] (GOVCERT.NL)
Sent: woensdag 19 januari 2011 14:23
To: [REDACTED]@vodafone.com
Cc: Cert Box; [REDACTED] (GOVCERT.NL)
Subject: Vodafone caller-ID spoofing

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Beste Ivor,

zoals telefonisch afgesproken nog even een mailtje.

Naar aanleiding van een blog post
(<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-for-authentication/>) heeft GOVCERT.NL een aantal testen uitgevoerd op Vodafone voicemail boxen van collega's. Middels services als spoofcard.com is het kinderlijk eenvoudig om een caller-ID te spoofen en vervolgens de voicemailboxen van willekeurige Vodafone klanten af te luisteren en instellingen te wijzigen. (tenzij de klant zelf een PIN-code heeft ingesteld wat vaak niet het geval is).

Bij andere providers lijkt dit niet te werken. Wanneer een Caller-ID niet vanaf het eigen netwerk naar de voicemailbox belt, wordt altijd om een wachtwoord/PIN gevraagd. Dit omdat er naast caller-ID ook op dergelijke spoofing wordt gecontroleerd.

GOVCERT.NL is bezig met het opstellen van een advies voor alle overheden met betrekking tot dit issue. Dit omdat Vodafone binnen steeds meer overheden gebruikt wordt. Wij zijn op zoek naar een contact persoon binnen Vodafone die een formeel antwoord kan geven op een aantal vragen die wij hebben naar aanleiding van onze eigen testen. Een antwoord dat wij vervolgens kunnen opnemen in ons uiteindelijke advies richting de overheid.

Alvast bedankt!
Met vriendelijke groeten,

[REDACTED]
security specialist

GOVCERT.NL
T +31 70 888 75 55
I www.govcert.nl
E [REDACTED]@govcert.nl

PGP Fingerprint: C87E 47E2 89D8 5DFB C86F A3F3 1557 E2E9 AC15 7DD5

GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government. We support the government in preventing and dealing with IT-related security incidents.

-----BEGIN PGP SIGNATURE-----
Version: PGP Desktop 9.8.3 (Build 4028)
Charset: utf-8

w1cDBQFNuwb9aHKK94RdvsRCKXPAP9wVxitRrNPxL7BK5UjsB/p2zNPOhPXrfI3
4zpJM1uSPAD9F3YEYNQSn2P5w7L0CEK+wAQXackKQS1NU/xF/nw6c1g=
=GEUs
-----END PGP SIGNATURE-----

VenJ-4-Vodafone voicemail eenvoudig af te luisteren-StLu

From: [REDACTED] (GOVCERT.NL)
Sent: woensdag 19 januari 2011 17:22
To: [REDACTED]@logius.nl
Cc: [REDACTED] (GOVCERT.NL)
Subject: Vodafone voicemail eenvoudig af te luisteren

Beste [REDACTED], zoals net besproken even een mailtje mbt het vodafone issue.

=====

Uit de testen blijkt dat het eenvoudig is om de voicemail boxen van willekeurige Vodafone gebruikers af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatie mechanisme gebruikt voor het beluisteren van de voicemail-box. Standaard wordt hierbij niet om een PIN code gevraagd. Het caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

Naar aanleiding van een Blog-post van 30-05-2010 (<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-for-authentication/>) heeft het beveiligingsbedrijf Fox-IT een aantal testen uitgevoerd op de beveiliging van voicemail op het Vodafone netwerk wat het bovenstaande bevestigt.

Daarnaast hebben wij zelf ook testen uitgevoerd en kunnen bevestigen dat dit werkt. Wij zijn op dit moment in afwachting van een formeel antwoord van Vodafone maar hebben dit nog niet gekregen.

Wij adviseren u na te gaan wie er binnen uw organisatie gebruik maakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. (Standaard staat hier geen PIN-code op).

=====

Hieronder mijn mail aan Vodafone ([REDACTED]@vodafone.com):

=====

Beste [REDACTED],

zoals telefonisch afgesproken nog even een mailtje.

Naar aanleiding van een blog post (<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-for-authentication/>) heeft GOVCERT.NL een aantal testen uitgevoerd op Vodafone voicemail boxen van collega's. Middels services als spoofcard.com is het kinderlijk eenvoudig om een caller-ID te spoofen en vervolgens de voicemailboxen van willekeurige Vodafone klanten af te luisteren en instellingen te wijzigen. (tenzij de klant zelf een PIN-code heeft ingesteld wat vaak niet het geval is).

Bij andere providers lijkt dit niet te werken. Wanneer een Caller-ID niet vanaf het eigen netwerk naar de voicemailbox belt, wordt altijd om een wachtwoord/PIN gevraagd. Dit omdat er naast caller-ID ook op dergelijke spoofing wordt gecontroleerd.

GOVCERT.NL is bezig met het opstellen van een advies voor alle overheden met betrekking tot dit issue. Dit omdat Vodafone binnen steeds meer overheden gebruikt wordt. Wij zijn op zoek naar een contact persoon binnen Vodafone die een formeel antwoord kan geven op een aantal vragen die wij hebben naar aanleiding van onze eigen testen. Een antwoord dat wij vervolgens kunnen opnemen in ons uiteindelijke advies richting de overheid.

Alvast bedankt!
Met vriendelijke groeten,
[REDACTED]

=====

--voor de duidelijkheid, wij hebben dus nog niets gecommuniceerd naar onze BVA's.

--
[REDACTED]

VenJ-4-Vodafone voicemail eenvoudig af te luisteren-StLu
security specialist

GOVCERT.NL
T +31 70 888 75 55
I www.govcert.nl
E [REDACTED]@govcert.nl

PGP Fingerprint: C87E 47E2 89D8 5DFB C86F A3F3 1557 E2E9 AC15 7DD5

GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government. We support the government in preventing and dealing with IT-related security incidents.

Van: Info GOVCERT.NL [info@govcert.nl]
Verzonden: vrijdag 21 januari 2011 15:04
Aan: lb@lists.govcert.nl; dsc@lists.govcert.nl; bva@govcert.nl
CC: [REDACTED]
Onderwerp: [IB-list] Vodafone voicemail eenvoudig af te luisteren

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Beste DSC-ers, IB-ers en Beveiligingsambtenaren,

Uit door ons geverifieerde testen blijkt dat het eenvoudig is om de voicemail boxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatie mechanisme gebruikt voor het beluisteren van de voicemail-box. Standaard wordt hierbij niet om een PIN code gevraagd, dit is een gebruikersinstelling. Het caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

Naar aanleiding van een Blog-post van medio vorig jaar
(<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id>
-fo

r-authentication/)

heeft het beveiligingsbedrijf Fox-IT een aantal testen uitgevoerd op de beveiliging van voicemail op het Vodafone netwerk wat het bovenstaande bevestigt.

Wij adviseren u na te gaan wie er binnen uw organisatie gebruik maakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. Om altijd naar uw PIN-code te laten vragen, belt u met 1233. In het menu kiest u vervolgens 2, 5, 3 en 1.

Zowel vanuit de contracthouder namens de Staat (SBO) en vanuit GOVCERT.NL is contact opgenomen met Vodafone. Als er hier meer informatie uit voortvloeit brengen we u op de hoogte.

Met vriendelijke groeten,
GOVCERT.NL

+----
GOVCERT.NL

Postbus 84011, 2508 AA Den Haag
+31 70 888 75 55 | www.govcert.nl | aart.jochem@govcert.nl

PGP Fingerprint: 0C37 1329 11F8 AFA7 C8FF 8319 EA0A EB03 0EC3 7CFC

GOVCERT.NL is het Cyber Security en Incident Response Team van de Nederlandse overheid. Wij ondersteunen overheidsorganisaties in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten.

+----
Het Nationaal Trendrapport Cybercrime en Digitale veiligheid 2010 is gepubliceerd. Kijk op:
<http://www.govcert.nl/trends>

+----

-----BEGIN PGP SIGNATURE-----

Version: PGP Desktop 9.8.3 (Build 4028)

Charset: utf-8

wlcDBQFNOZI09aHKK94RdvsRCIvnAP9N10eEDga2P76cnZObo94kDvesv/F9YaTf
bQgvapxXxwD+Iaq2TeZvrVktDpWIOpDTpZhuDPaXOZ0dk4m/sI+8at0=
=S1Yn

-----END PGP SIGNATURE-----

IB mailing list

IB@lists.govcert.nl

VenJ-8-RE Vodafone caller-ID spoofing
From: [REDACTED], VF-NL [REDACTED]@vodafone.com]
Sent: dinsdag 25 januari 2011 15:30
To: [REDACTED] (GOVCERT.NL)
Cc: [REDACTED], VF-NL; Cert Box; [REDACTED] (GOVCERT.NL)
Subject: RE: Vodafone caller-ID spoofing

Beste [REDACTED]

Zoals vanmorgen telefonisch besproken de reactie van Vodafone m.b.t. caller ID spoofing. Op basis van de melding van GovCert en de vragen die hieruit zijn voortgekomen, hebben we vanuit Vodafone de huidige mogelijkheden onderzocht en daarnaast gekeken naar netwerk verbeteringen die verzorgd kunnen worden om mogelijk misbruik van onze voicemail dienst op basis van 'spoofing' te voorkomen.

'Spoofing' is het imiteren van de 'caller ID/ A-nummer', waarbij contact gelegd wordt met de voicemaildienst van het betreffende A-nummer, waarmee het mogelijk zou zijn om direct toegang te krijgen tot de niet met een pincode beveiligde voicemaildienst van het A-nummer (Vodafone gebruikt A-nummer authenticatie om toegang tot de voicemaildienst te verkrijgen). Er worden via internet-providers "spoofing"-achtige diensten aangeboden.

Wat kan er op korte termijn verzorgd worden?

De huidige voicemaildienst voor onze corporate klanten voorziet in een optionele extra bescherming van de voicemaildienst door het beveiligen middels een verplichte pincode. Deze pincode staat momenteel default "uit", maar kan individueel, per eindgebruiker geactiveerd worden.

Via het IVR-menu, optie 2 - 5 - 3 - 1 "altijd vragen om pincode", kan deze extra beveiliging worden geactiveerd. Hiermee dient de eindgebruiker voor iedere keer dat hij/zij gebruik maakt van de voicemaildienst zijn/haar pincode te vermelden.

welke maatregelen worden er daarnaast in het netwerk verzorgd ?

Eventuele 'spoofing' kan alleen plaatsvinden, indien gesprekken buiten het Vodafone netwerk worden opgezet. Op dit moment onderzoeken we de mogelijkheden om gesprekken die buiten het Vodafone netwerk worden opgezet, waarbij de voicemail wordt uitgeluisterd standaard te voorzien van de vraag om de pincode te vermelden, alvorens gebruik te kunnen maken van de voicemaildienst. Het implementeren van deze optie, zorgt er wel voor dat onze klanten in het buitenland de pincode dienen in te voeren alvorens toegang te krijgen tot de voicemaildienst.

Daarnaast onderzoeken we, of bovenstaande wijziging verzorgd kan worden voor specifieke klanten(groep), en/of voor de gehele Vodafone klantengroep. Aangezien we tevens het vermoeden hebben dat klanten hun pincode wel eens vergeten, willen we tevens de mogelijkheid verzorgen om dit middels een sms bericht te ontvangen zodra je dit aangeeft bij het benaderen van de voicemaildienst.

De komende weken verkrijgen we meer duidelijkheid over de wijze waarop, en de bijbehorende doorlooptijd waarbinnen bovenstaande maatregelen in ons netwerk kunnen worden geïmplementeerd.

Mocht je n.a.v. bovenstaande nog vragen hebben dan hoor ik dat uiteraard graag.

Met vriendelijke groet,

[REDACTED]
[REDACTED]
Vodafone Technology

Tel: [REDACTED]
E-mail: [REDACTED]@vodafone.com
Web: www.vodafone.nl

Vodafone Netherlands
KvK-nummer 14052264
Avenue Ceramique 300, 6221 KX Maastricht Postbus 1500, 6201 BM Maastricht

VenJ-8-RE Vodafone caller-ID spoofing

(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

P Please consider the environment before printing this e-mail

-----Original Message-----

From: [REDACTED] (GOVCERT.NL) [mailto:[REDACTED]@govcert.nl]
Sent: woensdag 19 januari 2011 14:23
To: [REDACTED], VF-NL
Cc: GOVCERT.NL; [REDACTED] (GOVCERT.NL)
Subject: Vodafone caller-ID spoofing

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Beste [REDACTED],

zoals telefonisch afgesproken nog even een mailtje.

Naar aanleiding van een blog post

([http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-fo](http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-fo-r-authentication/)

r-authentication/) heeft GOVCERT.NL een aantal testen uitgevoerd op Vodafone voicemail boxen van collega's. Middels services als spoofcard.com is het kinderlijk eenvoudig om een caller-ID te spoofen en vervolgens de voicemailboxen van willekeurige Vodafone klanten af te luisteren en instellingen te wijzigen. (tenzij de klant zelf een PIN-code heeft ingesteld wat vaak niet het geval is).

Bij andere providers lijkt dit niet te werken. Wanneer een Caller-ID niet vanaf het eigen netwerk naar de voicemailbox belt, wordt altijd om een wachtwoord/PIN gevraagd. Dit omdat er naast caller-ID ook op dergelijke spoofing wordt gecontroleerd.

GOVCERT.NL is bezig met het opstellen van een advies voor alle overheden met betrekking tot dit issue. Dit omdat Vodafone binnen steeds meer overheden gebruikt wordt. Wij zijn opzoek naar een contact persoon binnen Vodafone die een formeel antwoord kan geven op een aantal vragen die wij hebben naar aanleiding van onze eigen testen. Een antwoord dat wij vervolgens kunnen opnemen in ons uiteindelijke advies richting de overheid.

Alvast bedankt!

Met vriendelijke groeten,

--

[REDACTED]
security specialist

GOVCERT.NL
T +31 70 888 75 55
I www.govcert.nl
E [REDACTED]@govcert.nl

PGP Fingerprint: C87E 47E2 89D8 5DFB C86F A3F3 1557 E2E9 AC15 7DD5

GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government. We support the government in preventing and dealing with IT-related security incidents.

VenJ-8-RE Vodafone caller-ID spoofing

-----BEGIN PGP SIGNATURE-----

Version: PGP Desktop 9.8.3 (Build 4028)

Charset: utf-8

wlcDBQFNuwb9aHKK94RdvsRCKXPAP9wVxitRrNPxL7BK5UjsB/p2zNPohPXrfI3
4zpJM1uSPAD9F3YEYNQSn2P5w7L0cEk+wAQXackKQS1NU/xF/nw6c1g=
=GEUS

-----END PGP SIGNATURE-----

Venj-12

Van: [REDACTED] (GOVCERT.NL) [REDACTED]@govcert.nl]

Verzonden: donderdag 27 januari 2011 15:35

Aan: exop@lists.govcert.nl

Onderwerp: [Exop] GOVCERT.NL-informatie over drie recente kwesties op hetterrein van ICT & Veiligheid

Urgentie: Hoog

Beste collega's,

De afgelopen dagen zijn er enkele kwesties in het nieuws gekomen op het terrein van ICT & Veiligheid. Hieronder treffen jullie korte GOVCERT.NL-informatie over die kwesties aan.

Reeds bekende OV-Chipkaart kwetsbaarheid nu volledig uitgebuit

Vandaag (27-1-2011) is er een Algemeen Overleg over de OV-chipkaart. Al langer is bekend dat de beveiliging van de Mifare-classic chip, die het hart vormt van de OV-chipkaart en ook in gebruik is in veel toegangspassen, gekraakt kan worden. GOVCERT.NL heeft in 2008 het overheidsdomein hierover geïnformeerd. Al vanaf 2008 is er soft- en hardware beschikbaar die het kraken mogelijk maakt. Deze software is nu zo ver ontwikkeld dat die niet alleen saldo naar een chipkaart kan schrijven, maar ook kan verhullen dat de kaart is gemanipuleerd: bij controles valt een fraudeur dus niet door de mand. Deze verder ontwikkelde software maakt het ook eenvoudiger om toegangspassen te manipuleren. Het is belangrijk om te beseffen dat er geen nieuwe lekken in de mifare chip ontdekt zijn; er is alleen makkelijker toegankelijke software beschikbaar gekomen. Overigens maakt de nieuwe Rijkspas geen gebruik van de Mifare-classic chip.

Door de toegenomen aandacht voor de OV-chipkaart zouden in eerste instantie bijvoorbeeld journalisten pogingen kunnen wagen om bij overheidsgebouwen binnen te komen.

Vodafone-voicemailboxen eenvoudig af te luisteren

Uit door GOVCERT.NL geverifieerde testen blijkt dat het eenvoudig is om de voicemailboxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatiemechanisme gebruikt voor het beluisteren van de voicemail-box. Dit caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

GOVCERT.NL heeft zijn contactpersonen (informatiebeveiligers en beveiligingsautoriteiten van de departementen) geadviseerd na te gaan wie er binnen hun organisaties gebruikmaakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. Standaard wordt namelijk niet om een PIN-code gevraagd: het instellen van een PIN-code is een gebruikersinstelling.

Zowel vanuit de contracthouder namens de Staat (SBO) als vanuit GOVCERT.NL is contact opgenomen met Vodafone. Alertheid is des te meer van belang, omdat de Rijksoverheid in 2011 voor telefonie overgaat naar Vodafone. Vodafone heeft aangegeven te onderzoeken welke oplossingsmogelijkheden er zijn voor het Vodafone-netwerk.

Online fraude met emissierechten

GOVCERT.NL werd in de afgelopen periode via haar securitynetwerk benaderd over een aanval op de gebruikers (via keylogging-malware) van de online CO₂-registers van de Nederlandse Emissieautoriteit (NEA). GOVCERT.NL heeft de NEA over deze aanval geïnformeerd, waarop de NEA maatregelen heeft genomen en haar Europese partners heeft ingelicht. Daarbij kwam naar voren dat kwaadwillenden intussen in andere landen CO₂-emissierechten hebben misbruikt als middel voor grootschalige fraude en diefstal. De Europese emissieautoriteiten hebben tot nader bericht hun online loketten gesloten.

De NEA is deelnemer geworden van GOVCERT.NL en ontvangt nu onze volledige dienstverlening

en adviezen. Hiermee kan de NEA haar dienstverlening/websites beter beveiligen en krijgt zij ondersteuning bij daadwerkelijke incidenten. GOVCERT.NL heeft de Europese collega-CERT's over de kwestie geïnformeerd.

Vriendelijke groet,

[Redacted signature]

GOVCERT.NL

T +31 70 888 7557

I www.govcert.nl

E [Redacted email]@govcert.nl

Postbus 84011, 2508 AA, Den Haag

NB Alleen voor intern gebruik Rijksoverheid

Venj-15

From: [REDACTED] (GOVCERT.NL)**Sent:** woensdag 2 februari 2011 11:30**To:** Waakdienst**Cc:** [REDACTED] (GOVCERT.NL)**Subject:** Fwd: Vodafone mail mailbox

Nice, op het VERA (intranet van obr.minbzk.nl, voormalig VROM onderdeel) is naar aanleiding van onze waarschuwing het volgende verschenen :

Dit is dus op VERA verschenen!

Zet een slot op je voicemail

Het blijkt redelijk eenvoudig te zijn de voicemailboxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren.

Die waarschuwing heeft GOVCERT, de expertorganisatie informatiebeveiliging van de overheid, onlangs uitgedaan. De meeste door voormalig VROM verstrekte mobiele telefoons en blackberries zijn van Vodafone. Wie zijn voicemailbox niet heeft beveiligd met een pincode, loopt het risico dat kwaadwillenden deze kunnen af luisteren.

Pincode

Iedere Vodafonegebruiker wordt daarom geadviseerd om direct een viercijferige PIN-code op de voicemailbox van zijn of haar mobiele telefoon te zetten. Om die in te stellen bel je met 1233 (daarvoor een 0 intoetsen!). In het menu kies je vervolgens 2, 5, 3 en tot slot een 1.

LET OP: lees voordat je aan de slag gaat eerst de handleiding van Vodafone (kijk bij de link hieronder). De instructies voor de PIN-code staan op pagina 10.

Aanvullend krijg je een dringend advies nooit vertrouwelijke mededelingen in te spreken als je wordt doorverbonden naar een voicemailbox.

-
- [Handleiding Vodafone](#)

door govcert

Van: [REDACTED] (GOVCERT.NL) [REDACTED]@govcert.nl

Verzonden: donderdag 3 februari 2011 12:22

Aan: [REDACTED]

Onderwerp: nieuwe informatie van Govcert

Dag [REDACTED]

Is het Expert Opinion produkt / verspreidingswijze ervan al besproken in het CBIB?

Hierbij het laatste produkt, in een iets andere vorm (meer een heads-up). Hij is eind vorige week al uitgegaan, maar ben helaas vergeten hem direct aan je door te sturen.

vr. groet,

Beste collega's,

De afgelopen dagen zijn er enkele kwesties in het nieuws gekomen op het terrein van ICT & Veiligheid. Hieronder treffen jullie korte GOVCERT.NL-informatie over die kwesties aan.

Reeds bekende OV-Chipkaart kwetsbaarheid nu volledig uitgebuit

Vandaag (27-1-2011) is er een Algemeen Overleg over de OV-chipkaart. Al langer is bekend dat de beveiliging van de Mifare-classic chip, die het hart vormt van de OV-chipkaart en ook in gebruik is in veel toegangspassen, gekraakt kan worden. GOVCERT.NL heeft in 2008 het overheidsdomein hierover geïnformeerd. Al vanaf 2008 is er soft- en hardware beschikbaar die het kraken mogelijk maakt. Deze software is nu zo ver ontwikkeld dat die niet alleen saldo naar een chipkaart kan schrijven, maar ook kan verhullen dat de kaart is gemanipuleerd: bij controles valt een fraudeur dus niet door de mand. Deze verder ontwikkelde software maakt het ook eenvoudiger om toegangspassen te manipuleren. Het is belangrijk om te beseffen dat er geen nieuwe lekken in de mifare chip ontdekt zijn; er is alleen makkelijker toegankelijke software beschikbaar gekomen. Overigens maakt de nieuwe Rijkspas geen gebruik van de Mifare-classic chip.

Door de toegenomen aandacht voor de OV-chipkaart zouden in eerste instantie bijvoorbeeld journalisten pogingen kunnen wagen om bij overheidsgebouwen binnen te komen.

Vodafone-voicemailboxen eenvoudig af te luisteren

Uit door GOVCERT.NL geverifieerde testen blijkt dat het eenvoudig is om de voicemailboxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatiemechanisme gebruikt voor het beluisteren van de voicemail-box. Dit caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

GOVCERT.NL heeft zijn contactpersonen (informatiebeveiligers en beveiligingsautoriteiten van de departementen) geadviseerd na te gaan wie er binnen hun organisaties gebruikmaakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. Standaard wordt namelijk niet om een PIN-code gevraagd: het instellen van een PIN-code is een gebruikersinstelling.

Zowel vanuit de contracthouder namens de Staat (SBO) als vanuit GOVCERT.NL is contact opgenomen met Vodafone. Alertheid is des te meer van belang, omdat de Rijksoverheid in 2011 voor telefonie overgaat naar Vodafone. Vodafone heeft aangegeven te onderzoeken welke oplossingsmogelijkheden er zijn voor het Vodafone-netwerk.

Online fraude met emissierechten

GOVCERT.NL werd in de afgelopen periode via haar securitynetwerk benaderd over een aanval

op de gebruikers (via keylogging-malware) van de online CO₂-registers van de Nederlandse Emissieautoriteit (NEA). GOVCERT.NL heeft de NEA over deze aanval geïnformeerd, waarop de NEA maatregelen heeft genomen en haar Europese partners heeft ingelicht. Daarbij kwam naar voren dat kwaadwillenden intussen in andere landen CO₂-emissierechten hebben misbruikt als middel voor grootschalige fraude en diefstal. De Europese emissieautoriteiten hebben tot nader bericht hun online loketten gesloten.

De NEA is deelnemer geworden van GOVCERT.NL en ontvangt nu onze volledige dienstverlening en adviezen. Hiermee kan de NEA haar dienstverlening/websites beter beveiligen en krijgt zij ondersteuning bij daadwerkelijke incidenten. GOVCERT.NL heeft de Europese collega-CERT's over de kwestie geïnformeerd.

Vriendelijke groet,

GOVCERT.NL

T +31 70 888 [REDACTED]

I www.govcert.nl

E [REDACTED]@govcert.nl

Postbus 84011, 2508 AA, Den Haag

NB Alleen voor intern gebruik Rijksoverheid

VenJ-17

Van: [REDACTED] - BD/DBOB/COZA

Verzonden: donderdag 24 maart 2011 10:35

Aan: [REDACTED] - BD/DII; [REDACTED] - BD/DI

Onderwerp: 2011-03-24 Afluisteren persoonlijke voicemailbox in de media...

Ter info en communicatie intern via o.a. CSB/CTB?

Contract- en Leveranciersmanager

Ministerie van Veiligheid en Justitie

Commerciële Zaken, Contractmanagement Justitie (CMJ)

Schedeldoekshaven 100 | 2511 EX | Den Haag | H-714

Postbus 20301 | 2500 EH | Den Haag

T 070 370 [REDACTED]

M [REDACTED]

[REDACTED]@minjus.nl

cmj@minjus.nl

<http://www.justitie.nl>

Justitie. Recht raakt mensen.

Denk aan het milieu en print dit bericht uitsluitend indien echt noodzakelijk

Van: [REDACTED] [mailto:[REDACTED]@getronics.com]

Verzonden: woensdag 23 maart 2011 21:11

Onderwerp: afluisteren persoonlijke voicemailbox in de media...

Geachte relatie,

Naar aanleiding van alle mediacommunicatie aangaande inbreuk op de Voicemailbox van mobiele gebruikers wil ik u bij deze informeren over de stand van zaken binnen KPN.

In de media wordt aangegeven dat het beluisteren van de mobiele voicemailbox vanaf een externe bestemming mogelijk is. Bijvoorbeeld vanaf een vaste telefoon.

De mogelijkheid om de persoonlijke voicemailbox vanaf een andere bestemming dan de mobiele telefoon te benaderen wordt ook door KPN ondersteund.

Nu is echter onlosmakelijk bewezen dat kwaadwillende deze voicemailbox kunnen benaderen en de berichten kunnen beluisteren en opslaan. (zie de link)

KPN reeds bij de introductie van deze dienst geconstateerd dat gebruikmakende van de standaard, bij de simkaart behorende pincode, niet voor afdoende beveiliging zorgt.

Vele mobiele gebruikers veranderen de persoonlijke pincode, behorende bij de simkaart, niet en blijft de standaard 0000 of in geval van Vodafone 3333 gehandhaafd.

En is dus de kans op inbreuk erg groot.

Na introductie van de dienst en de constatering dat inbreuk vrij eenvoudig was, heeft KPN Mobile meteen actie ondernomen en een oplossing geïmplementeerd.

Deze oplossing bestaat uit:

KPN koppelt aan elke 06 nummer een 6 cijferig random nummer, dus een uniek 6 cijferig nummer die alleen bij de mobiele gebruiker bekend is, voor bellen naar de persoonlijke voicemailbox vanaf een bestemming anders

dan het mobiele netwerk van KPN.

Hierdoor is het dus voor buitenstaanders/kwaadwillende onmogelijk om de persoonlijke voicemailbox van derden met standaard codes uit te kunnen luisteren en worden zaken/problemen, zoals nu worden blootgelegd in de media, dus voorkomen.

Vertrouwende u hiermee geïnformeerd en gerust gesteld te hebben zodat u weer kunt blijven vertrouwen op de dienstverlening van KPN.

<http://www.eenvandaag.nl/>

Unclassified

Met vriendelijke groet,

[REDACTED]

[REDACTED]

[REDACTED]

Mobile Voice & Data Solutions



Röntgenlaan 75
2719 DX Zoetermeer
Postbus 2
2700 AA Zoetermeer

mobile +31 (0) [REDACTED]

email: [REDACTED]@getronics.com

Getronics Nederland BV, Handelsregister 34.115.845 Amsterdam

The information transmitted is intended only for use by the addressee and may contain confidential and/or privileged material. Any review, re-transmission, dissemination or other use of it, or the taking of any action in reliance upon this information by persons and/or entities other than the intended recipient is prohibited. If you received this in error, please inform the sender and/or addressee immediately and delete the material. Thank you

[REDACTED]
[REDACTED]
Van: [REDACTED] (GOVCERT.NL) [REDACTED]@govcert.nl]
Verzonden: donderdag 24 maart 2011 14:42
Aan: [REDACTED]
Onderwerp: Overzicht handelingen met betrekking tot Voicemailincident en uitleg 2 kwetsbaarheden

Tijdelijk Vodafone voicemail incident

19 januari 2011

GOVCERT.NL wordt door een vertrouwde partij uit haar netwerk geattendeerd op een openbaar artikel op het Internet. Daarin wordt een methode beschreven waarmee Vodafone voicemail kan worden afgeluisterd. De vertrouwde partij geeft aan deze methode onderzocht te hebben. Deze blijkt te werken. Dit wordt aan GOVCERT.NL meegedeeld met de vraag of GOVCERT.NL daarmee iets kan doen richting (rijks)overheid. GOVCERT.NL heeft nog dezelfde dag de methode getest en is tot dezelfde conclusie gekomen. Vervolgens vraagt GOVCERT.NL zich af of dit een typisch probleem is voor het Vodafone netwerk of dat dit ook op andere netwerken een probleem is. Deze vraag wordt voorgelegd aan een vertrouwde persoon uit het netwerk van GOVCERT.NL, die bij KPN belast is met veiligheid van het mobiele verkeer. Deze contactpersoon meldt dat KPN maatregelen heeft getroffen om deze vorm van misbruik te voorkomen. Vervolgens neemt GOVCERT.NL contact op met Vodafone en meldt het probleem. Vodafone geeft aan het probleem te zullen onderzoeken. De melding wordt vanuit GOVCERT.NL geëscaleerd naar de directeur van Logius GOVCERT.NL is onderdeel van dit agentschap van BZK. De directeur is vervolgens gaan escaleren.

21 januari 2011

De directeur van Logius besluit dat het moment gekomen is dat GOVCERT.NL haar deelnemers moet informeren. GOVCERT.NL informeert de technisch contactpersonen, de informatiebeveiligers en de BVA's van alle deelnemers dezelfde middag nog per e-mail over het probleem en de oplossing. GOVCERT.NL adviseert daarin om alle Vodafone voicemailboxen zo in te stellen dat deze voorzien is van een pincode én dat Vodafone voicemail altijd deze pincode vraagt. Ook de juiste menukeuzes daarvoor worden in de e-mail genoemd.

Het advies van GOVCERT.NL had de problemen kunnen voorkomen die gepresenteerd werden in de uitzending van EenVandaag op 23 maart 2011. Het advies biedt ook bescherming tegen een andere, nog niet in de pers gepubliceerde aanvalsmethode op Vodafone voicemailboxen. De twee methodes worden hierna aan u uitgelegd.

24/03/2011 12:40

Twee kwetsbaarheden

Wij zijn bekend met twee kwetsbaarheden in de beveiliging van Vodafone-voicemail. Een van deze twee kwetsbaarheden is op woensdag 23 maart jl. in de media gekomen. Hieronder een korte uiteenzetting van de twee kwetsbaarheden, en aanvullende informatie over gevolgen voor derde partijen.

Kwetsbaarheid 1: (zoals in de media bekend)

Wanneer men de voicemail wil afluisteren vanaf een ander toestel dan de eigen mobiel (bijvoorbeeld vanaf een vaste lijn), dan kan dit door naar een speciaal nummer van Vodafone te bellen (+31 654 501 233). Wanneer dit nummer wordt gebeld, vraagt de computer vervolgens om het mobiele nummer op te geven van de voicemail die men wil beluisteren en om de PIN-code. Wanneer er nooit een PIN-code op de voicemail is geplaatst, is deze code standaard 3333.

In de media is deze kwetsbaarheid aangetoond bij de voicemaildienst van Vodafone. Het is niet uitgesloten dat een dergelijke kwetsbaarheid ook bij andere telecomproviders voorkomt. Wij hebben dit vooralsnog niet onderzocht.

Oplossing:

Vodafone heeft nu het beluisteren van de voicemail box, vanaf een vaste lijn, uitgeschakeld wanneer er nooit een

PIN-code geplaatst is door de eindgebruiker. PIN 3333 werkt dus niet meer. Advies blijft om in het instellingen menu te kiezen voor de optie "Vraag altijd om een PIN-code".

Kwetsbaarheid 2: (zoals eerder in januari door oa Fox-IT en GOVCERT.NL aangetoond)

Als men vanaf de eigen mobiele telefoon, de voicemail van Vodafone belt (+31 654 501 233), vraagt de dienst standaard nooit om een pin-code. Vodafone stelt op basis van de zogenaamde 'caller-ID' (het nummer waarmee gebeld wordt) vast wie er belt en welke voicemailbox daarbij hoort. Echter, er bestaan diensten zoals Skype maar ook online diensten als spoofcard.com waarmee men elk willekeurig caller-id kan nadoen. Je kunt hiermee dus jezelf voordoen als iemand anders en zijn of haar voicemail af luisteren zonder dat er om een PIN-code wordt gevraagd.

Deze methode om voicemail van een ander af te luisteren, werkt ook nu nog na de maatregelen die Vodafone heeft getroffen om kwetsbaarheid 1 te verhelpen.

Wij hebben destijds onderzocht of deze kwetsbaarheid alleen bij Vodafone speelt door onder andere contact op te nemen met KPN. KPN heeft ons meegedeeld dat zij niet kwetsbaar waren voor deze aanvalstechniek. Vooralsnog lijkt het er dus op dat alleen het netwerk van Vodafone deze kwetsbaarheid bevat.

Oplossing:



GOVCERT.NL heeft haar deelnemers op 21 januari ingelicht over deze kwetsbaarheid. Wij hebben daarbij een advies gegeven waarmee iedereen zichzelf kan beschermen. Ons advies is om in het instellingenmenu te kiezen voor de optie "Vraag altijd om een PIN-code". Iedereen die dit advies destijds had opgevolgd, was nu niet kwetsbaar geweest voor deze kwetsbaarheid, en was ook niet kwetsbaar geweest voor kwetsbaarheid 1. Ons advies was een effectieve maatregel tegen beide kwetsbaarheid.

Echter: de echte oplossing voor kwetsbaarheid 2 ligt bij Vodafone zelf. Dit zal waarschijnlijk om een investering vragen daar software en apparatuur zal moeten worden aangepast.

Mogelijke gevolgen voor derde partijen:

We vermoeden dat er organisaties zijn, in andere andere de financiële sector, die personen identificeren (mede) op basis van het caller-ID. Zoals hierboven beschreven kan een caller-ID door iedereen nagedaan worden en is dit op zichzelf staand dus geen goede methode om iemand te identificeren. Wij hebben dit op dit moment in onderzoek.

Van: [REDACTED] (GOVCERT.NL) [REDACTED]@govcert.nl
Verzonden: vrijdag 25 maart 2011 10:38
Aan: All GovCert
CC: [REDACTED]
Onderwerp: Factsheet en WD-artikel over Vodafone-Issue
Bijlagen: FS-2011-02 Kwetsbaarheden in voicemaildiensten 1.1.pdf



FS-2011-02
wetsbaarheden in v.
All,

Naar aanleiding van de ontwikkelingen van gisteren en afgelopen nacht hebben we de factsheet die klaarstond aangepast. Deze nieuwe versie (1.1) heb ik bij deze mail gevolgd.

 Ik ga nu:

1. DSC/IB/BVA mailen
2. Factsheet plaatsen op govcert.nl (over ongeveer 10 minuten)
3. Artikel op waarschuwingdienst.nl plaatsen (over ongeveer 30 minuten)

[REDACTED]
GOVCERT.NL
T +31 70 888 75 65
I www.govcert.nl
E [REDACTED]@govcert.nl
PGP Fingerprint: [REDACTED]

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.

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.

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 af luisteren 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.

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

Wilhelms van Prutenweg 104
2585 AN Den Haag

Postbus 96810
2509 JE Den Haag

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

Moet u zelf nog iets doen?

Vodafone heeft de twee kwetsbaarheden verholpen. Ons advies, dat wij eerder aan onze deelnemers gaven, blijft echter van kracht.

Wij adviseren iedereen (ongeacht uw telecomprovider) om de eigen voicemail zo in te stellen dat:

1. Er nooit gebruik wordt gemaakt van een standaard pincode, maar altijd van een eigen pincode.
2. Er *altijd* naar een pincode wordt gevraagd, ook als u vanaf uw eigen mobiele telefoon belt om uw voicemail te beluisteren.

Als u gebruik maakt van Vodafone als telecomprovider, dan kunt u dit instellen door 1233 te bellen, en in het menu te kiezen voor optie 2, gevolgd door 5, 3 en 1. Voor andere telecomproviders kunnen deze instellingen en menu-opties anders zijn.

Het instellen van uw voicemail zoals hierboven beschreven heeft dus als effect dat u altijd een pincode zult moeten invoeren om uw voicemail te beluisteren, ook als u gewoon binnen Nederland en vanaf uw eigen telefoon belt.

Is deze informatie alleen relevant voor klanten van Vodafone?

De informatie in deze factsheet is mogelijk ook relevant voor klanten van andere telecomproviders, maar dit hebben wij nog niet kunnen bevestigen.

Wij raden iedereen dan ook aan het advies in deze factsheet zo goed mogelijk op te volgen, ongeacht de gebruikte telecomprovider (zie hiervoor het kopje "Moet u zelf nog iets doen?").

Een goede pincode:

Een pincode is goed als u hem gemakkelijk kunt onthouden en een ander hem moeilijk kan raden.

Hieronder een korte opsomming van getallen die wij in ieder geval afraden als pincode:

- Een standaard pincode (die u niet zelf heeft gekozen)
- Geboortedata van uzelf of familie
- Postcodes van uw woning of werk
- Cijferreeksen, zoals 1234
- Volledige herhalingen, zoals 1111



Van: Info GOVCERT.NL [info@govcert.nl]
Verzonden: vrijdag 25 maart 2011 10:53
Aan: dsc@lists.govcert.nl; ib@lists.govcert.nl; bva@govcert.nl
CC: [redacted]@mininv.nl; [redacted]@minvws.nl; [redacted]@tweedekamer.nl;
 [redacted]@minbuza.nl; [redacted]@minfin.nl; [redacted]@mindef.nl;
 [redacted]@minvenw.nl; [redacted]@minez.nl; [redacted]@minjus.nl;
 [redacted]@minocw.nl; [redacted]@minszw.nl; [redacted]@minvrom.nl; [redacted]@minaz.nl;
 [redacted]@minvenw.nl
Onderwerp: [IB-list] Factsheet: kwetsbaarheden in voicemaildiensten



FS-2011-02



ATT21307523.txt

wetsbaarheden in v.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Beste IB'ers, DSC'ers en BVA's,

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 +31 70 888 75 65
 I www.govcert.nl
 E [redacted]@govcert.nl
 PGP Fingerprint: [redacted]

GOVCERT.NL is the Cyber Security & Incident Response Team for the Dutch Government. We support 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

wj8DBQFNjGXTvCQ2rBBFEzMRAsOIAJ9060RxZJ7WygXPgsZuHRHvXI2uOACfUvJM
 xmVdU20WpyZSTuw6xKcupl0=
 =27wn

-----END PGP SIGNATURE-----

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.

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 af luisteren 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.

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

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

Moet u zelf nog iets doen?

Vodafone heeft de twee kwetsbaarheden verholpen. Ons advies, dat wij eerder aan onze deelnemers gaven, blijft echter van kracht.

Wij adviseren iedereen (ongeacht uw telecomprovider) om de eigen voicemail zo in te stellen dat:

1. Er nooit gebruik wordt gemaakt van een standaard pincode, maar altijd van een eigen pincode.
2. Er altijd naar een pincode wordt gevraagd, ook als u vanaf uw eigen mobiele telefoon belt om uw voicemail te beluisteren.

Als u gebruik maakt van Vodafone als telecomprovider, dan kunt u dit instellen door 1233 te bellen, en in het menu te kiezen voor optie 2, gevolgd door 5, 3 en 1. Voor andere telecomproviders kunnen deze instellingen en menu-opties anders zijn.

Het instellen van uw voicemail zoals hierboven beschreven heeft dus als effect dat u altijd een pincode zult moeten invoeren om uw voicemail te beluisteren, ook als u gewoon binnen Nederland en vanaf uw eigen telefoon belt.

Is deze informatie alleen relevant voor klanten van Vodafone?

De informatie in deze factsheet is mogelijk ook relevant voor klanten van andere telecomproviders, maar dit hebben wij nog niet kunnen bevestigen.

Wij raden iedereen dan ook aan het advies in deze factsheet zo goed mogelijk op te volgen, ongeacht de gebruikte telecomprovider (zie hiervoor het kopje "Moet u zelf nog iets doen?").

Een goede pincode:

Een pincode is goed als u hem gemakkelijk kunt onthouden en een ander hem moeilijk kan raden.

Hieronder een korte opsomming van getallen die wij in ieder geval afraden als pincode:

- Een standaard pincode (die u niet zelf heeft gekozen)
- Geboortedata van uzelf of familie
- Postcodes van uw woning of werk
- Cijferreeksen, zoals 1234
- Volledige herhalingen, zoals 1111

GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid. Vragen over de inhoud van deze factsheet kunt u richten aan info@govcert.nl of telefonisch via 070-8887555.



Deze factsheet is gepubliceerd onder de voorwaarden beschreven in de Creative Commons Naamsvermelding-Niet-commercieel-Gelijk delen 3.0 Nederland licentie.

ATT21307523.txt

IB mailing list
IB@lists.govcert.nl

[REDACTED]
Van: [REDACTED] BD/BSG/BVA [REDACTED]@minjus.nl
Verzonden: vrijdag 25 maart 2011 11:20
Aan: [REDACTED] BD/BSG/BVA; [REDACTED] - BD/BSG/BVA; [REDACTED]
[REDACTED] BD/BSG/BVA; [REDACTED] BD/BSG/BVA
CC: [REDACTED] BD/BSG
Onderwerp: FW: Vodafone voicemail eenvoudig af te luisteren
Urgentie: Hoog

Ha collega's,

Wij waren met de problematiek bekend en hebben dat direct/tijdig - zie onderstaande mail - onder de aandacht gebracht van GDI.

[REDACTED]

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 ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Veiligheid en Justitie

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 risks inherent in the electronic transmission of messages.

Ministry of Security and Justice

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

Van: [REDACTED] - GDI
Verzonden: zondag 23 januari 2011 21:01
Aan: [REDACTED] - GDI/FO/PM; [REDACTED] - GDI/BV; [REDACTED]
[REDACTED] - GDI/BV
Cc: [REDACTED] - GDI/FO/PM; [REDACTED] - BD/BSG/BVA
Onderwerp: FW: Vodafone voicemail eenvoudig af te luisteren

[REDACTED]

Kan jij dit in het migratie project meenemen als vereiste.

Met vriendelijke groet,

[REDACTED]
Directeur GDI

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

Van: [REDACTED] - BD/BSG/BVA
Verzonden: vrijdag 21 januari 2011 15:57
Aan: [REDACTED] - GDI
Onderwerp: FW: Vodafone voicemail eenvoudig af te luisteren

Neem aan dat jij deze mail ook binnen krijgt.

Goed weekend,

[REDACTED]

:
: -----Oorspronkelijk bericht-----

Van: Info GOVCERT.NL [mailto:info@govcert.nl]
Verzonden: vrijdag 21 januari 2011 15:04
Aan: Ib@lists.govcert.nl; dsc@lists.govcert.nl; bva@govcert.nl
CC: [REDACTED]
Onderwerp: Vodafone voicemail eenvoudig af te luisteren

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Beste DSC-ers, IB-ers en Beveiligingsambtenaren,

Uit door ons geverifieerde testen blijkt dat het eenvoudig is om de voicemail boxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatie mechanisme gebruikt voor het beluisteren van de voicemail-box. Standaard wordt hierbij niet om een PIN code gevraagd, dit is een gebruikersinstelling. Het caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

Naar aanleiding van een Blog-post van medio vorig jaar
(<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id-fo>

-authentication/)
heeft het beveiligingsbedrijf Fox-IT een aantal testen uitgevoerd op de beveiliging van voicemail op het Vodafone netwerk wat het bovenstaande bevestigt.

Wij adviseren u na te gaan wie er binnen uw organisatie gebruik maakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. Om altijd naar uw PIN-code te laten vragen, belt u met 1233. In het menu kiest u vervolgens 2, 5, 3 en 1.

Zowel vanuit de contracthouder namens de Staat (SBO) en vanuit GOVCERT.NL is contact opgenomen met Vodafone. Als er hier meer informatie uit voortvloeit brengen we u op de hoogte.

Met vriendelijke groeten,
GOVCERT.NL

+---
GOVCERT.NL

Postbus 84011, 2508 AA Den Haag
+31 70 888 75 55 | www.govcert.nl | [REDACTED]@govcert.nl

PGP Fingerprint: 0C37 1329 11F8 AFA7 C8FF 8319 EA0A EB03 0EC3 7CFC

GOVCERT.NL is het Cyber Security en Incident Response Team van de Nederlandse overheid. Wij ondersteunen overheidsorganisaties in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten.

+---
Het Nationaal Trendrapport Cybercrime en Digitale veiligheid 2010 is gepubliceerd.
Kijk op: <http://www.govcert.nl/trends>
+---

-----BEGIN PGP SIGNATURE-----

Version: PGP Desktop 9.8.3 (Build 4028)
Charset: utf-8

wlcDBQFNOZI09aHKK94RdvsRCIvNAP9N10eEDga2P76cnZObo94kDvesv/F9YaTf
bQgvapxXxwD+Iaq2TeZvrVktDpWlOpDTpZhuDPaXOZ0dk4m/s1+8at0=
=S1Yn

-----END PGP SIGNATURE-----

Van: [REDACTED]
Verzonden: vrijdag 25 maart 2011 12:05
Aan: [REDACTED]
Onderwerp: FW: [IB-list] Factsheet: kwetsbaarheden in voicemaildiensten



FS-2011-02 ATT21307489.txt
wetsbaarheden in v. (151 B)

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

Van: Info GOVCERT.NL [mailto:info@govcert.nl]
Verzonden: vrijdag 25 maart 2011 10:53
Aan: dsc@lists.govcert.nl; ib@lists.govcert.nl; bva@govcert.nl
CC: [REDACTED]@minlnv.nl; [REDACTED]@minvws.nl; [REDACTED]@tweedekamer.nl;
[REDACTED]@minbuza.nl; [REDACTED]@minfin.nl; [REDACTED]@mindef.nl;
[REDACTED]@minvenw.nl; [REDACTED]@minez.nl; [REDACTED]@minjus.nl;
[REDACTED]@minocw.nl; [REDACTED]@minszw.nl; [REDACTED]@minvrom.nl; [REDACTED]@minaz.nl;
[REDACTED]@minvenw.nl
Onderwerp: [IB-list] Factsheet: kwetsbaarheden in voicemaildiensten

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

Beste IB'ers, DSC'ers en BVA's,

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 +31 70 888 75 65
L www.govcert.nl
E [REDACTED]@govcert.nl
PGP Fingerprint: [REDACTED]

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

wj8DBQFNjGXTvCQ2rBBFEzMRAsOIAJ9060RxZJ7WygXPgsZuHRHvXl2uOACfUvJM
xmVdU20WpyZSTuw6xKcup10=
=27wn

-----END PGP SIGNATURE-----

Verj - 28
B35

[REDACTED]
Van: [REDACTED]
Verzonden: vrijdag 25 maart 2011 12:17
Onderwerp: FW: [IB-list] Factsheet: kwetsbaarheden in voicemaildiensten



FS-2011-02
wetsbaarheden in v. Ter info...

Met vriendelijke groet,
[REDACTED]

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.

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 af luisteren 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.

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

Wilhelmina van Pruisenweg 104
2585 AN Den Haag

Postbus 96810
2509 JE Den Haag

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

Moet u zelf nog iets doen?

Vodafone heeft de twee kwetsbaarheden verholpen. Ons advies, dat wij eerder aan onze deelnemers gaven, blijft echter van kracht.

Wij adviseren iedereen (ongeacht uw telecomprovider) om de eigen voicemail zo in te stellen dat:

1. Er nooit gebruik wordt gemaakt van een standaard pincode, maar altijd van een eigen pincode.
2. Er *altijd* naar een pincode wordt gevraagd, ook als u vanaf uw eigen mobiele telefoon belt om uw voicemail te beluisteren.

Als u gebruik maakt van Vodafone als telecomprovider, dan kunt u dit instellen door 1233 te bellen, en in het menu te kiezen voor optie 2, gevolgd door 5, 3 en 1. Voor andere telecomproviders kunnen deze instellingen en menu-opties anders zijn.

Het instellen van uw voicemail zoals hierboven beschreven heeft dus als effect dat u altijd een pincode zult moeten invoeren om uw voicemail te beluisteren, ook als u gewoon binnen Nederland en vanaf uw eigen telefoon belt.

Is deze informatie alleen relevant voor klanten van Vodafone?

De informatie in deze factsheet is mogelijk ook relevant voor klanten van andere telecomproviders, maar dit hebben wij nog niet kunnen bevestigen.

Wij raden iedereen dan ook aan het advies in deze factsheet zo goed mogelijk op te volgen, ongeacht de gebruikte telecomprovider (zie hiervoor het kopje "Moet u zelf nog iets doen?").

Een goede pincode:

Een pincode is goed als u hem gemakkelijk kunt onthouden en een ander hem moeilijk kan raden.

Hieronder een korte opsomming van getallen die wij in ieder geval afraden als pincode:

- Een standaard pincode (die u niet zelf heeft gekozen)
- Geboortedata van uzelf of familie
- Postcodes van uw woning of werk
- Cijferreeksen, zoals 1234
- Volledige herhalingen, zoals 1111



VenJ-30

[REDACTED]
Van: [REDACTED]@GOVCERT.NL ([REDACTED]@govcert.nl)

Verzonden: vrijdag 25 maart 2011 13:29

Aan: exop@lists.govcert.nl

Onderwerp: [Exop] Expert Opinion ICT&Veiligheid d.d. 25 maart 2011

—BEGIN PGP SIGNED MESSAGE—

Hash: SHA256

Geachte collega's,

Hierbij treft u een nieuwe Expert Opinion ICT & Veiligheid aan over drie onderwerpen.

1. RSA en Comodo: gerichte digitale aanvallen
2. SCADA kwetsbaarheden inclusief exploitcode gepubliceerd
3. Afluisteren Vodafone-mailboxen

Met vriendelijke groet,

[REDACTED]
[REDACTED]
T 070 888 [REDACTED]
I www.govcert.nl
E [REDACTED]@govcert.nl
PGP Fingerprint: [REDACTED]

Het nieuwe jaaroverzicht van GOVCERT.NL is gepubliceerd. Zie:
<http://www.govcert.nl/render.html?it=177>

GOVCERT.NL is het Computer Emergency Response Team van en voor de Nederlandse overheid. Wij ondersteunen overheidsorganisaties in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten. GOVCERT.NL maakt onderdeel uit van Logius en bouwt mee aan de e-overheid.

—BEGIN PGP SIGNATURE—

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

wlcDBQFNjlp19aHKK94RdvsRCIkEAP99xC2tAQk2wTL4Av8YAaji88CgPxU5Uwv
0WRq2zaUKAD7BG/YJUgUu4L//u5lgsKM8w/D/OoTkZIAdyB+tR3Dq9A=
=Jcwe

—END PGP SIGNATURE—

Enkele actuele ontwikkelingen op het terrein van ICT & Veiligheid

1. RSA en Comodo: gerichte digitale aanvallen

Twee beveiligingsbedrijven (RSA en Comodo) zijn onlangs langs digitale weg aangevallen en bestolen.

RSA is een Amerikaans beveiligingsbedrijf. Een bekend produkt van RSA is de SecureID "two-factor" authenticatiemethode: het werken met tokens om – bijvoorbeeld – veilig transacties te doen of email te versturen. RSA heeft bekend gemaakt dat onlangs langs digitale weg gevoelige informatie over RSA SecureID is gestolen. RSA waarschuwt klanten, dat het uitlekken van gegevens over RSA SecureID-implementaties kan leiden tot een verminderde effectiviteit van deze wijze van "two-factor" authenticatie. Over de details van deze aanval of de impact ervan is op dit moment nog weinig bekend.

In dezelfde periode is beveiligingsbedrijf Comodo slachtoffer geworden van een aanval. Comodo is een beveiligingsbedrijf dat onder andere SSL-certificaten uitdeelt, waarmee websites/webverkeer kan worden beveiligd, via https en het bekende "slotje". Onlangs zijn door kwaadwillenden op de systemen van Comodo enkele certificaten aangemaakt. Het betrof certificaten voor o.a. Google, Yahoo, en Windows Live. Een dergelijk certificaat is ideaal om 'man-in-the-middle' te spelen: het afvangen van internetverkeer (*content*), omdat de aanvalleur tussen bijvoorbeeld Google en de gebruiker in kan gaan zitten. De certificaten zijn niet van echte certificaten te onderscheiden.

Beide aanvallen (gerichte aanvallen, tegenwoordig vaak ook bestempeld als *Advanced Persistent Threat*) moeten op ingenieuze wijze hebben plaatsgevonden, mogelijk in combinatie met social engineering. Beveiliging is namelijk de core-business van de beide bedrijven.

De 'buit' is in beide gevallen niet rechtstreeks renderend. Het vermoeden is dan ook, dat in beide gevallen de buit benut wordt als bouwsteen voor een grotere aanval of voor andere acties. Het is niet duidelijk of er een relatie tussen de twee incidenten bestaat. Wel geven de digitale inbraken opnieuw aan, dat niemand zich onkwetsbaar moet achten als het om dergelijke aanvallen gaat.

Over daders of actoren is relatief weinig bekend. Wel zou de aanval richting Comodo vanaf een IP-adres in Iran hebben plaatsgevonden en zouden de aangemaakte certificaten op een systeem in Iran aangetroffen zijn en. Dit sluit andere actoren echter niet uit.

2. SCADA-kwetsbaarheden inclusief exploitcode gepubliceerd

De belangstelling in de community van ICT-security-onderzoekers voor kwetsbaarheden in SCADA/procescontrolesystemen neemt opnieuw zichtbaar toe. Een bevestiging van de ontwikkeling die al eerder gesignaleerd is in het Nationaal Trendrapport Cybercrime en Digitale Veiligheid. Deze week is namelijk een groot aantal kwetsbaarheden in SCADA/procescontrole-software bekend gemaakt door verschillende onderzoekers. Slechts in één geval gebeurde dit langs de weg van 'responsible disclosure' (zie EXOP 21-2-2011, item nr. 3).

Het gaat in totaal om 36 kwetsbaarheden in 6 verschillende procescontroleproducten. In bijna alle gevallen is het voor kwaadwillenden mogelijk om zelf code te laten uitvoeren op de systemen waarop de SCADA software draait. De exploitcode om dit te kunnen doen hebben de onderzoekers (op één geval na) ook beschikbaar gesteld. Wat de eventuele risico's en gevolgen kunnen zijn voor procesbesturingen hangt af van de exacte configuraties en eventuele reeds getroffen beveiligingsmaatregelen.

Met veruit de meeste beschikbaar gestelde exploitcodes is het niet mogelijk direct besturingscommandos's aan te passen en daarmee de bestuurd processen te manipuleren. Wél kunnen de systemen die de operators overzichts informatie geven uitvallen. Dit kan leiden tot een gedeeltelijke of volledige *loss of view*. Voor 5 van de 6 kwetsbare SCADA-producten zijn nog geen patches beschikbaar gesteld. De kans is aanwezig dat met name hackers uit nieuwsgierigheid en scriptkiddies op zoek zullen gaan naar kwetsbare systemen.

Voor een tweetal andere kwetsbaarheden en bijbehorende exploits geldt dat kwaadwillenden direct toegang kunnen krijgen tot de SCADA-systemen en uiteindelijk de besturing kunnen overnemen. Voor deze kwetsbaarheden is (nog) geen update/patch beschikbaar gesteld. Of, en zo ja, wanneer deze zullen komen is niet bekend. Ook is onbekend of antivirus-software de gepubliceerde exploits kan herkennen.

3. Afluisteren Vodafone-mailboxen

Begin 2011 berichtte GOVCERT.NL dat uit geverifieerde testen bleek dat het eenvoudig is om de voicemailboxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Woensdag 23 en donderdag 24 maart jl. zijn twee kwetsbaarheden in de media gekomen.

Op www.waarschuwingsdienst.nl staat de meest actuele informatie van GOVCERT.NL.

Daarnaast is er ook een factsheet gepubliceerd, welke online te vinden is op: <http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemailediensten.html>

We vermoeden dat er organisaties zijn, onder andere in de financiële sector, die personen identificeren (mede) op basis van het caller-ID. Zoals op www.waarschuwingsdienst.nl beschreven kan een caller-ID door iedereen *gespoofed*/nagedaan worden. Het is dus - op zichzelf staand - geen goede methode om iemand te identificeren. GOVCERT.NL heeft dit momenteel in onderzoek.

De Govcert-deelnemers en ISAC's worden steeds geïnformeerd over de voor hen relevante informatie.

GOVCERT.NL, 26 maart 2011

VERSIE 1.0

T +31 70 888 75 55 / I www.govcert.nl / E info@govcert.nl

ATT21347760.txt

Dit is de Expert Opinion ICT&veiligheid mailinglijst van Govcert.nl
Voor vragen info@govcert.nl of 070-8887555

Van: [REDACTED] (GOVCERT.NL) [info@govcert.nl]
 Verzonden: vrijdag 25 maart 2011 14:20
 Aan: info@govcert.nl
 Onderwerp: [IB-list] End-of-Week



ATT21367210.txt

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Beste DSC-ers en IB-ers,

Het zal niemand ontgaan zijn dat er deze week het een-en-ander te doen was om kwetsbaarheden in het voicemailstelsel van Vodafone. Op woensdag deed het TV-programma EenVandaag al uit de doeken hoe het mogelijk was om voicemails van Vodafoneklanten af te luisteren door misbruik te maken van een standaard pincode [1]. GOVCERT.NL waarschuwde in januari van dit jaar al voor problemen met Vodafone voicemail, hetgeen op donderdag door EenVandaag werd bevestigd [2]. Nieuwsuur maakte het verhaal compleet door te demonstreren dat het, op basis van 'caller-ID spoofing' mogelijk bleek om zelfs zonder pincode een voicemailbox af te luisteren [3]. Het issue dat Nieuwsuur demonstreerde was overigens het issue waarvoor wij in januari specifiek een waarschuwing uitstuurden.

Voor meer informatie verwijst ik u naar de diverse communicatie-uitingen die wij vandaag over dit onderwerp hebben verstuurd zoals een factsheet [4], een e-mail aan DSC-ers, IB-ers en BVA's en een bericht op Waarschuwingsdienst.nl [5].

[1] <http://www.eenvandaag.nl/swf/player.swf?videoID=97518&external=0>

[2] <http://www.eenvandaag.nl/swf/player.swf?videoID=97532&external=0>

[3] <http://nieuwsuur.nl/uitzending/2011-03-24/>

[4] <http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemailediensten.html>

[5] <https://www.waarschuwingsdienst.nl/Risicos/Kwetsbaarheden/Kwetsbaarheden+in+voicemailediensten.html>

Verstuurde beveiligingsadviezen

GOVCERT.NL-2010-163 [v1.03][H/M] Kwetsbaarheden in HP OpenView
 Network Node Manager

GOVCERT.NL-2010-208 [v1.01][H/M] Kwetsbaarheden verholpen in HP
 Network Node manager GOVCERT.NL-2010-227 [v1.08][L/M] Meerdere
 kwetsbaarheden opgelost in
 LibPNG

GOVCERT.NL-2010-259 [v1.02][M/M] Kwetsbaarheden opgelost in HP
 Network Node Manager GOVCERT.NL-2010-259 [v1.03][H/M] Kwetsbaarheden
 opgelost in HP

Network Node Manager GOVCERT.NL-2010-281 [v1.02][M/M] Kwetsbaarheid in
 HP OpenView Network
 Node Manager verholpen GOVCERT.NL-2010-281 [v1.03][H/M] Kwetsbaarheid
 in HP OpenView Network
 Node Manager verholpen GOVCERT.NL-2010-499 [v1.02][L/M] FreeType update
 verhelpt twee

kwetsbaarheden GOVCERT.NL-2011-023 [v1.01][M/M] HP update verhelpt

HP OpenView Network Node Manager GOVCERT.NL-2011-023 [v1.02][H/M] HP
 update verhelpt kwetsbaarheden in

HP OpenView Network Node Manager GOVCERT.NL-2011-100 [v1.03][M/H]

Update voor Samba verhelpt
in LibTIFF kwetsbaarheid GOVCERT.NL-2011-106 [v1.03][M/M] Kwetsbaarheid verholpen

verhelpt bibliotheek GOVCERT.NL-2011-108 [v1.02][M/H] Update voor subversion

STARTTLS kwetsbaarheid GOVCERT.NL-2011-110 [v1.01][M/H] Kwetsbaarheid in

in Adobe Flash, Reader implementaties gevonden GOVCERT.NL-2011-129 [v1.01][H/M] Kwetsbaarheid

Adobe Flash, Reader en Acrobat gevonden GOVCERT.NL-2011-129 [v1.02][H/M] Kwetsbaarheid in

voor en Acrobat gevonden GOVCERT.NL-2011-131 [v1.00][M/H] RSA waarschuwt

PHP verhelpt kwetsbaarheden met PHP veiligheidsprobleem met RSA SecurID GOVCERT.NL-2011-132 [v1.00][M/H]

5.3.6 GOVCERT.NL-2011-133 [v1.00][M/H] Ubuntu verhelpt meerdere

Kwetsbaarheden in Wireshark kwetsbaarheden in Linux kernel GOVCERT.NL-2011-134 [v1.00][M/M]

GOVCERT.NL-2011-134 [v1.01][M/M] Kwetsbaarheden in Wireshark

GOVCERT.NL-2011-134 [v1.02][M/M] Kwetsbaarheden in Wireshark

GOVCERT.NL-2011-134 [v1.03][M/M] Kwetsbaarheden in Wireshark

GOVCERT.NL-2011-135 [v1.00][M/H] Apple verhelpt groot aantal

kwetsbaar bij verwerken kwetsbaarheden in Mac OS X GOVCERT.NL-2011-136 [v1.00][H/M] RealPlayer

Firefox blokkeert IVR-bestanden GOVCERT.NL-2011-137 [v1.00][M/H] Lotus Domino bevat

blokken frauduleuze authenticatiekwetsbaarheid GOVCERT.NL-2011-138 [v1.00][M/H] Update voor

Symantec certificaten GOVCERT.NL-2011-138 [v1.01][M/H] Updates

certificaten GOVCERT.NL-2011-139 [v1.00][M/M] CSRF-kwetsbaarheid in

LiveUpdate Administrator GOVCERT.NL-2011-140 [v1.00][M/M] Kwetsbaarheid

verholpen in Libtiff GOVCERT.NL-2011-141 [v1.00][M/H] Denial of Service Kwetsbaarheid

gevonden in PHP GOVCERT.NL-2011-142 [v1.00][M/M] VLC update verhelpt

kwetsbaarheden GOVCERT.NL-2011-143 [v1.00][M/M] Update voor Apache verhelpt

kwetsbaarheid GOVCERT.NL-2011-144 [v1.00][M/H] Zero-day kwetsbaarheid in

P Data Protector

Nieuw op de kennisbank (<https://kennisbank.govcert.nl>)

* 2010 Internet Crime Report

Het gezamenlijke jaarverslag van het Internet Crime Complaint Center (IC3) van de FBI en het National White Collar Crime Center (NW3C). De top drie van klachten/meldingen bestaat uit: 1. Niet leveren van goederen of betalingen; 2. Scams waarin de naam van de FBI wordt misbruikt; en 3. Identiteitsdiefstal. Ondanks het feit dat het een buitenlands rapport betreft, geeft het een goed beeld (en trendontwikkeling) van de oplichtingspraktijken die door 'cybercriminelen' worden gebruikt.

* Applications of Modern Cryptography - Technologies, applications and choices

Dit Engelstalig whitepaper van Surfnets geeft een inleiding (basisniveau) tot cryptografie, de (laatste) technische stand van zaken op het gebied van cryptografie en een overzicht van real-world applicaties die in uw eigen praktijk kunnen worden toegepast.

Wat was er nog meer in het nieuws =====

* 'Serieuze cyberaanval' op Europese Unie

Voorafgaand aan een belangrijke Europese bespreking hebben ict-aanvallen plaatsgevonden op de

Europese Commissie en de External Action Service [6]. Bronnen bij de EU typeren de aanvallen als 'a big one' en 'widespread'. Details over de aanvallen ontbreken echter. Als maatregel is de toegang tot e-mail en intranet alleen nog mogelijk vanuit het interne netwerk en is medewerkers gevraagd hun wachtwoord te wijzigen.

[6] <http://euobserver.com/9/32049>

*** Frauduleuze Comodo-certificaten in omloop**

Naar deze week bleek, heeft certificaatprovider Comodo circa twee weken geleden 9 SSL-certificaten verstrekt die het niet had mogen uitgeven [7, 8]. Hoewel Comodo het incident naar eigen zeggen snel opmerkte en direct browserleveranciers en domeineigenaren inlichtte, was het kwaad op dat moment al geschied. Met de frauduleuze certificaten is het mogelijk om gebruikers gevoelige informatie te ontfutselen via phishing en Man-in-the-Middle (MitM) aanvallen. De frauduleuze SSL-certificaten richtten zich op grote bedrijven als Yahoo, Skype, Microsoft en Google.

De aanval bleek mogelijk nadat een gebruikersnaam met bijbehorend wachtwoord van een Comodo Trusted Partner in handen was gevallen van een kwaadwillende. Op basis van deze gegevens was het mogelijk om op afstand willekeurige certificaten te ondertekenen met de Comodo-CA.

Hoewel de frauduleuze certificaten direct op blacklists zijn geplaatst (CRL/OCSP) kan het gebeuren dat browsers deze toch accepteren als ze een CRL of OCSP niet kunnen benaderen. Vandaar dat diverse leveranciers updates uitbrachten om de certificaten lokaal in de browser of het besturingssysteem te blokkeren. Zie GOVCERT.NL-2011-138 en ons artikel op Waarschuwingsdienst.nl [9] voor meer informatie.

[7] <http://blogs.comodo.com/it-security/data-security/the-recent-ca-compromise/>

[8] <http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>

[9] <https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2011-027.html>

*** Kwaadwillenden bemachtigen informatie over RSA SecurID**

Naast de EU en Comodo bleek deze week ook nog een derde partij succesvol aangevallen te zijn: RSA. Via een 'zeer geavanceerde' aanval wisten kwaadwillenden binnen te dringen op het netwerk van dit beveiligingsbedrijf [10]. Volgens RSA zijn de kwaadwillenden erin geslaagd om informatie te verzamelen over de RSA SecurID-oplossing. Hoewel ernstig, verwacht RSA niet dat de kwaadwillenden deze informatie kunnen misbruiken om succesvolle aanvallen uit te voeren op SecurID-installaties.

[10] <http://www.rsa.com/node.aspx?id=3872>

*** Groot aantal 0-day kwetsbaarheden in SCADA-software bekend gemaakt** Deze week hebben een aantal security-onderzoekers, onafhankelijk van elkaar, 36 0-day kwetsbaarheden in SCADA-software gepubliceerd. Tevens hebben ze in 35 gevallen ook exploitcode beschikbaar gesteld. De belangstelling in de community van ICT-securityonderzoekers voor kwetsbaarheden in SCADA/procescontrolesystemen neemt dus opnieuw zichtbaar toe. Een bevestiging van de ontwikkeling die we al eerder beschreven in het Nationaal Trendrapport Cybercrime en Digitale Veiligheid.

De kwetsbaarheden zijn gevonden in de volgende producten: Siemens Factorylink, ICONICS Genesis, 7-technologies IGGS, DATAC Realwin, Advantech Broadwin webaccess en IntegraXor.

SCADA-software is niet opgenomen in de foto daarom schrijven we niet specifiek voor dergelijke producten. Onze collega's van ICS-CERT/US-CERT hebben hierover een aantal alerts gepubliceerd [11].

[11] http://www.us-cert.gov/control_systems/

Tot slot nog een tip om snel geld te verdienen als u nog een IPv4-blok op de planken heeft liggen. Want met de enorme schaarste aan IPv4-adressen blijkt hier een handel in te ontstaan. Zo heeft Microsoft deze week 666.624 IP-adressen overgenomen van het failliete Nortel voor een totaalbedrag van \$7,5 miljoen [11]. Kosten per IP-adres: \$11,25!

[11] http://blog.internetgovernance.org/blog/_archives/2011/3/23/4778509.html

Ik wens u heel fijn weekend dat helaas een uur korter dan normaal is!

Met vriendelijke groet,


Security Specialist

GOVCERT.NL
T +31 70 888 75 55
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.

-----BEGIN PGP SIGNATURE-----

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

wlcDBQFNjJaB9aHKK94RdvsRCCZsAP9Ltszu7ZJYHhW2+5VVfHZW3eZiGI2e+Y9I
5nA8tfF2AQD/biB/aq/Y2ZsXabL5L727w0wZGsTJ3Kn7xfQGygbb9YE=
=1z11

-----END PGP SIGNATURE-----

[REDACTED]
Van: [REDACTED] (GOVCERT.NL) [REDACTED]@govcert.nl]

Verzonden: maandag 28 maart 2011 12:51

Aan: [REDACTED]

Onderwerp: FW: Brief aan Tweede Kamer inz Vodafone kwetsbaarheden

Bijlagen: Vodafone - brief TK.PDF

Beste Steven,

Zie onderstaande mail aan de medewerkers van GOVCERT.NL.
Per abuis ben ik je vergeten in de maillijst te zetten. Mijn excuses.

Met vriendelijke groet,

[REDACTED]
[REDACTED]
GOVCERT.NL

T +31 70 888 75 55

I www.govcert.nl

E naam@govcert.nl

Wilhelmina van Pruysenweg 104

Postbus 84011

2508 AA Den Haag

GOVCERT.NL is het Cyber Security & Incident Response Team van de Nederlandse overheid. Wij ondersteunen overheidsorganisaties en organisaties met een publieke taak in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten.

From: [REDACTED] (GOVCERT.NL) On Behalf Of [REDACTED] (GOVCERT.NL)

Sent: maandag 28 maart 2011 9:27

To: Alle medewerkers GOVCERT.NL

Subject: Brief aan Tweede Kamer inz Vodafone kwetsbaarheden

Beste medewerkers,

Dit is de brief die minister Donner aan de Tweede Kamer heeft gestuurd naar aanleiding van het Vodafone voicemail incident. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Groet,

[REDACTED]
[REDACTED]
GOVCERT.NL

T +31 70 888 75 55

I www.govcert.nl

E [REDACTED]@govcert.nl

Wilhelmina van Pruysenweg 104

Postbus 96810

2509 JE Den Haag

GOVCERT.NL is het Cyber Security & Incident Response Team van de Nederlandse overheid. Wij ondersteunen overheidsorganisaties en organisaties met een publieke taak in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten.

28-3-2011



**Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties**

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten Generaal

DGBOB/DIR

**Schedeldoekshaven 200
2511 EZ Den Haag**

**Postbus 20011
2500 EA Den Haag**

www.dijksoverheid.nl

**Contactpersoon
Frank Heijgers**

**T (070) 428 8581
frank.heijgers@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 voicemailstelsel 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.

Datum
24 maart 2011

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 glisteren 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

Ven J-37

[REDACTED]
Van: [REDACTED]

Verzonden: maandag 28 maart 2011 15:56

Aan: [REDACTED]

CC: [REDACTED]

Onderwerp: FW: Kwas gena's

Heren,

excuus. in de vorige mail waren niet de laatste versie opgenomen van de vragen mbt vodafone. Vraag hierbij. Is het bv nog zinvol om te verwijzen/noemen campagne digibewust e.d..

Groet [REDACTED]

Ministerie van Veiligheid en Justitie
Directie Nationale Veiligheid

Schedeldoekshaven 200 2511 EZ Den Haag Kamer H 1420
Postbus 20011 2500 EA Den Haag

T: 0031 70 426 [REDACTED]

M: [REDACTED]

F: 0031 70 426 [REDACTED]

[REDACTED]@minbzk.nl

www.nationale-veiligheid.nl

Vraag en antwoord

Onderwerp	Kwas
Dossierhouder	[REDACTED]
Bereikbaarheid	[REDACTED]
Minister	Minister VenJ

Vraag

- **Welke relatie heeft dossier spionage/kwas met de beveiligingslek Vodafone? (Voortouw Vadofone/voicemail ligt bij BZK/Donner)**

Antwoord

Er is geen relatie, maar het beveiligingslek van Vodafone zorgt helaas wel voor een extra makkelijke toegang tot informatie en dat maakt spionage ook makkelijker. Deze kwestie is een illustratie van het dilemma tussen gebruikersgemak en beveiliging. Het toont aan dat we allemaal bereid moeten zijn om iets meer handelingen te verrichten. Maar het illustreert ook de verantwoordelijkheid van de gebruiker (om de instellingen aan te passen) en het gebrek aan bewustzijn over de daadwerkelijke (on)veiligheid van gebruikte techniek.

Vraag en antwoord

Onderwerp	Kwas
Dossierhouder	[REDACTED]
Bereikbaarheid	[REDACTED]
Minister	Minister BZK

Vraag

- **Welke maatregelen worden door het ministerie ondernomen nav beveiligingslek Vodafone? (Voortouw Vadofone/voicemail ligt bij BZK/minister Donner)**

Antwoord

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.

Over de kwestie Vodafone en het afluisteren van voicemails op afstand heeft mijn collega Donner u schriftelijk geïnformeerd (en een spoeddebat heeft hierover plaatsgevonden). Als gevolg van dit incident laat mijn collega Donner onderzoeken of er misbruik is gemaakt van deze fout en, indien daartoe aanleiding bestaat, in hoeverre staatsveiligheid in het geding is geweest. Voorts laat collega Donner onderzoeken op welke wijze de signaleringen van GovCERT actiever opgepakt kunnen worden. De uitkomsten hiervan zal betrokken worden bij het inrichten van de ICT-beveiligingsorganisatie.

[REDACTED]

Van: [REDACTED] - BD/DI
Verzonden: dinsdag 29 maart 2011 14:12
Aan: [REDACTED] BD/DII; [REDACTED] - BD/DII
Onderwerp: FW: Vodafone voicemail eenvoudig af te luisteren

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

Van: [REDACTED] - BD/DI
Verzonden: donderdag 24 maart 2011 15:11
Aan: 'OT2010'
Onderwerp: FW: Vodafone voicemail eenvoudig af te luisteren

[REDACTED]

Dit is de problematiek die ik vanmiddag nog eens aanhaalde. Onderstaand is aangegeven dat SBO contact is opgenomen met Vodafone. Is hier nu in het verlengde van het gebeuren van gisteren al meer nieuws over.

Groet,

[REDACTED]

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

Van: [REDACTED] - BD/DI
Verzonden: maandag 24 januari 2011 10:40
Aan: 'OT2010'
CC: [REDACTED] - BD/DI
Onderwerp: Vodafone voicemail eenvoudig af te luisteren

[REDACTED]

Zie onderstaand bericht. Mogelijk is dit afgelopen donderdag al aan de orde geweest. Zo ja, dan hoor ik dat wel tijdens onze meeting.
Zo nee, dan verneem ik graag wat met Vodafone hieromtrent is afgesproken.

Groet,

[REDACTED]

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

Van: Info GOVCERT.NL [mailto:info@govcert.nl]
Verzonden: vrijdag 21 januari 2011 15:04
Aan: Ib@lists.govcert.nl; dsc@lists.govcert.nl; bva@govcert.nl
CC: [REDACTED]
Onderwerp: Vodafone voicemail eenvoudig af te luisteren

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Beste DSC-ers, IB-ers en Beveiligingsambtenaren,

Uit door ons geverifieerde testen blijkt dat het eenvoudig is om de voicemail boxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Dit is mogelijk omdat Vodafone standaard alleen het caller-ID (het mobiele nummer) van de beller als authenticatie mechanisme gebruikt voor het beluisteren van de voicemail-box. Standaard wordt hierbij niet om een PIN code gevraagd, dit is een gebruikersinstelling. Het caller-ID is echter makkelijk te spoofen (imiteren). Er bestaan diverse diensten op het internet die caller-ID-spoofing aanbieden.

Naar aanleiding van een Blog-post van medio vorig jaar (<http://blog.hendricksen.eu/2010/05/30/vodafone-voicemail-uses-caller-id>

-fo
r-authentication/)
heeft het beveiligingsbedrijf Fox-IT een aantal testen uitgevoerd op de beveiliging van voicemail op het Vodafone netwerk wat het bovenstaande bevestigt.

Wij adviseren u na te gaan wie er binnen uw organisatie gebruik maakt van Vodafone en deze gebruikers te adviseren een PIN-code te zetten op de voicemail-box. Om altijd naar uw PIN-code te laten vragen, belt u met 1233.

In het menu kiest u vervolgens 2, 5, 3 en 1.

Zowel vanuit de contracthouder namens de Staat (SBO) en vanuit GOVCERT.NL is contact opgenomen met Vodafone. Als er hier meer informatie uit voortvloeit brengen we u op de hoogte.

Met vriendelijke groeten,
GOVCERT.NL

+---
GOVCERT.NL

Postbus 84011, 2508 AA Den Haag
+31 70 888 75 55 | www.govcert.nl | govcert@govcert.nl

PGP Fingerprint: [REDACTED]

GOVCERT.NL is het Cyber Security en Incident Response Team van de Nederlandse overheid. Wij ondersteunen overheidsorganisaties in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten.

+----
Het Nationaal Trendrapport Cybercrime en Digitale veiligheid 2010 is gepubliceerd. Kijk op:
<http://www.govcert.nl/trends>
+-----

-----BEGIN PGP SIGNATURE-----
Version: PGP Desktop 9.8.3 (Build 4028)
Charset: utf-8

wlcDBQFNOZI09aHKK94RdvsRCIvnAP9N10eEDga2P76cnZObo94kDvesv/F9YaTf
bQgvapxXxD+Iaq2TeZvrVktDpWIOpDTpZhuDPaXOZ0dk4m/sI+8at0=
=S1Yn

-----END PGP SIGNATURE-----

[REDACTED]

Van: [REDACTED]

Verzonden: dinsdag 29 maart 2011 16:06

Aan: [REDACTED]

Onderwerp: FW: spoeddebat

TKN

Met vriendelijke groet,

[REDACTED]
senior beleidsmedewerker

.....
Ministerie van BZK

Directoraat Generaal Organisatie en Bedrijfsvoering Rijk

Directie Informatiseringsbeleid Rijk

Schedeldoekshaven 200 | 2511 EZ | Den Haag | H1013

Postbus 20011 | 2500 EA | Den Haag

.....
T (070) 4268581

[REDACTED]@minbzk.nl

<http://www.minbzk.nl>

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

Van: [REDACTED] (GOVCERT.NL) [mailto:[REDACTED]@govcert.nl]

Verzonden: maandag 28 maart 2011 17:12

Aan: [REDACTED]

CC: [REDACTED] (GOVCERT.NL)

Onderwerp: spoeddebat

Dag [REDACTED]

Ik ben beschikbaar morgen als liaison voor het spoeddebat, samen met Erik de Jong. Kan evt. op de publieke tribune zitten of in de ambtenarenkamer (als ik aangemeld wordt) om antwoorden te genereren.

groet,
[REDACTED]

[REDACTED]
GOVCERT.NL

T +31 70 888 [REDACTED]

I www.govcert.nl

E [REDACTED]@govcert.nl

Postbus 84011, 2508 AA, Den Haag

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

GOVCERT.NL is het Cyber Security & Incident Response Team van de Nederlandse overheid. Wij ondersteunen overheidsorganisaties en organisaties met een publieke taak in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten.

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.

[REDACTED]

Van: [REDACTED]

Verzonden: woensdag 30 maart 2011 11:30

Aan: [REDACTED]

Onderwerp: FW: [Exop] Expert Opinion ICT&Veiligheid d.d. 25 maart 2011

Deze hebben jullie ook?

Groet,

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

Van: [REDACTED] (GOVCERT.NL) [mailto:[REDACTED]@govcert.nl]

Verzonden: vrijdag 25 maart 2011 13:29

Aan: exop@lists.govcert.nl

Onderwerp: [Exop] Expert Opinion ICT&Veiligheid d.d. 25 maart 2011

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Geachte collega's,

Hierbij treft u een nieuwe Expert Opinion ICT & Veiligheid aan over drie onderwerpen.

1. RSA en Comodo: gerichte digitale aanvallen
2. SCADA kwetsbaarheden inclusief exploitcode gepubliceerd
3. Afluisteren Vodafone-mailboxen

Met vriendelijke groet,

[REDACTED]
Manager Nieuwe Diensten

T 070 888 [REDACTED]

I www.govcert.nl

E [REDACTED]@govcert.nl

PGP Fingerprint: [REDACTED]

Het nieuwe jaaroverzicht van GOVCERT.NL is gepubliceerd. Zie:

<http://www.govcert.nl/render.html?it=177>

GOVCERT.NL is het Computer Emergency Response Team van en voor de Nederlandse overheid. Wij ondersteunen overheidsorganisaties in het voorkomen en afhandelen van ICT gerelateerde veiligheidsincidenten. GOVCERT.NL maakt onderdeel uit van Logius en bouwt mee aan de e-overheid.

-----BEGIN PGP SIGNATURE-----

Version: PGP Desktop 10.1.1 (Build 10)

Charset: utf-8

wlcDBQFNjlp19aHKK94RdvsRCIkEAP99xC2tAQk2wTLa4Av8YAaji88CgPxU5Uvw
0WRq2zaUKAD7BG/YJUgUu4L//u5lgsKM8w/D/OoTkZIAdyB+tR3Dq9A=

=Jcwe

-----END PGP SIGNATURE-----

Enkele actuele ontwikkelen op het terrein van ICT & Veiligheid

1. RSA en Comodo: gerichte digitale aanvallen

Twee beveiligingsbedrijven (RSA en Comodo) zijn onlangs langs digitale weg aangevallen en bestolen.

RSA is een Amerikaans beveiligingsbedrijf. Een bekend produkt van RSA is de SecureID "two-factor" authenticatiemethode: het werken met tokens om – bijvoorbeeld – veilig transacties te doen of email te versturen. RSA heeft bekend gemaakt dat onlangs langs digitale weg gevoelige informatie over RSA SecureID is gestolen. RSA waarschuwt klanten, dat het uitlekken van gegevens over RSA SecureID-implementaties kan leiden tot een verminderde effectiviteit van deze wijze van "two-factor" authenticatie. Over de details van deze aanval of de impact ervan is op dit moment nog weinig bekend.

In dezelfde periode is beveiligingsbedrijf Comodo slachtoffer geworden van een aanval. Comodo is een beveiligingsbedrijf dat onder andere SSL-certificaten uitgeeft, waarmee websites/webverkeer kan worden beveiligd, via https en het bekende "slotje". Onlangs zijn door kwaadwillenden op de systemen van Comodo enkele certificaten aangemaakt. Het betrof certificaten voor o.a. Google, Yahoo, en Windows Live. Een dergelijk certificaat is ideaal om 'man-in-the-middle' te spelen: het afvangen van internetverkeer (*content*), omdat de aanvaller tussen bijvoorbeeld Google en de gebruiker in kan gaan zitten. De certificaten zijn niet van echte certificaten te onderscheiden.

Beide aanvallen (gerichte aanvallen, tegenwoordig vaak ook bestempeld als *Advanced Persistent Threat*) moeten op ingenieuze wijze hebben plaatsgevonden, mogelijk in combinatie met social engineering. Beveiliging is namelijk de core-business van de beide bedrijven.

De 'buit' is in beide gevallen niet rechtstreeks renderend. Het vermoeden is dan ook, dat in beide gevallen de buit benut wordt als bouwsteen voor een grotere aanval of voor andere acties. Het is niet duidelijk of er een relatie tussen de twee incidenten bestaat. Wel geven de digitale inbraken opnieuw aan, dat niemand zich onkwetsbaar moet achten als het om dergelijke aanvallen gaat.

Over daders of actoren is relatief weinig bekend. Wel zou de aanval richting Comodo vanaf een IP-adres in Iran hebben plaatsgevonden en zouden de aangemaakte certificaten op een systeem in Iran aangetroffen zijn en. Dit sluit andere actoren echter niet uit.

2. SCADA-kwetsbaarheden inclusief exploitcode gepubliceerd

De belangstelling in de community van ICT-security-onderzoekers voor kwetsbaarheden in SCADA/procescontrolesystemen neemt opnieuw zichtbaar toe. Een bevestiging van de ontwikkeling die al eerder signaleerd is in het Nationaal Trendrapport Cybercrime en Digitale Veiligheid. Deze week is namelijk een groot aantal kwetsbaarheden in SCADA/procescontrole-software bekend gemaakt door verschillende onderzoekers. Slechts in één geval gebeurde dit langs de weg van 'responsible disclosure' (zie EXOP 21-2-2011, item nr. 3).

Alleen voor intern gebruik Rijksoverheid - Expert Opinion ICT & Veiligheid 25-03-2011

Het gaat in totaal om 36 kwetsbaarheden in 6 verschillende procescontroleproducten. In bijna alle gevallen is het voor kwaadwillenden mogelijk om zelf code te laten uitvoeren op de systemen waarop de SCADA software draait. De exploitcode om dit te kunnen doen hebben de onderzoekers (op één geval na) ook beschikbaar gesteld. Wat de eventuele risico's en gevolgen kunnen zijn voor procesbesturingen hangt af van de exacte configuraties en eventuele reeds getroffen beveiligingsmaatregelen.

Met veruit de meeste beschikbaar gestelde exploitcodes is het niet mogelijk direct besturingscommandos's aan te passen en daarmee de bestuurde processen te manipuleren. Wél kunnen de systemen die de operators overzichts informatie geven uitvallen. Dit kan leiden tot een gedeeltelijke of volledige *loss of view*. Voor 5 van de 6 kwetsbare SCADA-producten zijn nog geen patches beschikbaar gesteld. De kans is aanwezig dat met name hackers uit nieuwsgierigheid en scriptkiddies op zoek zullen gaan naar kwetsbare systemen.

Voor een tweetal andere kwetsbaarheden en bijbehorende exploits geldt dat kwaadwillenden direct toegang kunnen krijgen tot de SCADA-systemen en uiteindelijk de besturing kunnen overnemen. Voor deze kwetsbaarheden is (nog) geen update/patch beschikbaar gesteld. Of, en zo ja, wanneer deze zullen komen is niet bekend. Ook is onbekend of antivirus-software de gepubliceerde exploits kan herkennen.

3. Afluisteren Vodafone-mailboxen

Begin 2011 berichtte GOVCERT.NL dat uit geverifieerde testen bleek dat het eenvoudig is om de voicemailboxen van willekeurige gebruikers van Vodafone mobiele telefonie af te luisteren. Woensdag 23 en donderdag 24 maart jl. zijn twee kwetsbaarheden in de media gekomen.

Op www.waarschuwingsdienst.nl staat de meest actuele informatie van GOVCERT.NL.

Daarnaast is er ook een factsheet gepubliceerd, welke online te vinden is op: <http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemaildiensten.html>

We vermoeden dat er organisaties zijn, onder andere in de financiële sector, die personen identificeren (mede) op basis van het caller-ID. Zoals op www.waarschuwingsdienst.nl beschreven kan een caller-ID door iedereen *gespoofed*/nagedaan worden. Het is dus - op zichzelf staand - geen goede methode om iemand te identificeren. GOVCERT.NL heeft dit momenteel in onderzoek.

De Govcert-deelnemers en ISAC's worden steeds geïnformeerd over de voor hen relevante informatie.

GOVCERT.NL, 26 maart 2011

VERSIE 1.0

T +31 70 888 75 55 / I www.govcert.nl / E info@govcert.nl

Alleen voor intern gebruik Rijksoverheid - Expert Opinion ICT & Veiligheid 26-03-2011

ATT686931.txt

Dit is de Expert Opinion ICT&veiligheid mailinglijst van Govcert.nl
voor vragen info@govcert.nl of 070-8887555

Ven-42

Van: [REDACTED] (GOVCERT.NL) [info@govcert.nl]
Verzonden: vrijdag 1 april 2011 15:32
Aan: info@govcert.nl
Onderwerp: [IB-list] End-of-Week



ATT2441893.txt

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Beste DSC-ers en IB-ers,

Op 19 april vindt het tweede DSC-Overleg van dit jaar plaats in de Kromhout Kazerne in Utrecht. We hebben nog niet van iedereen een aan- of afmelding ontvangen voor deze bijeenkomst. Graag horen wij voor 5 april of u het DSC overleg wilt bijwonen. Vergeet niet uw kenteken even aan ons door te geven als u van plan bent om met de auto naar het overleg te komen.

Naar aanleiding van de kwetsbaarheden in de Vodafone voicemail heeft Minister Donner vorige week in een brief laten weten dat hij laat onderzoeken hoe de adviezen van GOVCERT.NL beter opgepakt kunnen worden. Er wordt nog onderzocht of er berichten zijn gelekt die de staatsveiligheid in het geding hebben gebracht.

Verstuurde beveiligingsadviezen

=====

GOVCERT.NL-2007-221 [v1.01][L/H] Cisco VPN client maakt
SYSTEM-rechten mogelijk GOVCERT.NL-2010-494 [v1.07][M/H] Update verhelpt
kwetsbaarheden in
Bind
GOVCERT.NL-2011-055 [v1.03][M/H] Update voor Tomcat verhelpt
kwetsbaarheden GOVCERT.NL-2011-093 [v1.03][M/H] Denial of Service
kwetsbaarheid in
BIND
GOVCERT.NL-2011-108 [v1.03][M/H] Update voor subversion verhelpt
kwetsbaarheid GOVCERT.NL-2011-130 [v1.02][M/H] Kwetsbaarheid in Kerberos
verholpen GOVCERT.NL-2011-133 [v1.01][M/H] Ubuntu verhelpt meerdere
kwetsbaarheden in Linux kernel GOVCERT.NL-2011-138 [v1.02][M/H] Updates
blokkeren frauduleuze
certificaten GOVCERT.NL-2011-140 [v1.01][M/M] Kwetsbaarheid verholpen in
Libtiff GOVCERT.NL-2011-142 [v1.01][H/M] VLC update verhelpt kwetsbaarheden GOVCERT.NL-2011-
145 [v1.00][M/M] Kwetsbaarheid gevonden in Safari
voor iPhone iOS GOVCERT.NL-2011-146 [v1.00][M/H] Citrix verhelpt
kwetsbaarheid in
Presentation en XenApp Server GOVCERT.NL-2011-147 [v1.00][M/H]
Kwetsbaarheden verholpen in libvirt GOVCERT.NL-2011-147 [v1.01][M/H] Kwetsbaarheden verholpen
in libvirt GOVCERT.NL-2011-148 [v1.00][L/M] Race-conditie in GNOME Display
Manager (GDM) verholpen GOVCERT.NL-2011-148 [v1.01][L/M] Race-conditie
in GNOME Display
Manager (GDM) verholpen GOVCERT.NL-2011-149 [v1.00][M/H] Meerdere
kwetsbaarheden verholpen in
PHP
GOVCERT.NL-2011-150 [v1.00][M/M] Xpdf kwetsbaar bij verwerken 'Type 1
fonts'
GOVCERT.NL-2011-151 [v1.00][M/M] VMWare verhelpt kwetsbaarheid in
vmrun utility GOVCERT.NL-2011-151 [v1.01][M/M] VMWare verhelpt
kwetsbaarheid in
vmrun utility GOVCERT.NL-2011-152 [v1.00][M/H] IBM verhelpt kwetsbaarheid
in IBM

kwetsbaarheid in

Secure Access Control System (ACS)

Nieuw op de kennisbank (<https://kennisbank.govcert.nl>)

=====

* Overzicht GOVCERT.NL Advisories Maart 2011

Dit is het overzicht van de door GOVCERT.NL verstuurde advisories in maart 2011, in csv-formaat

* The underground economy of spam

Deze bijdrage geeft een compleet overzicht van een grootschalig botnet vanuit het perspectief van de botmaster en benadrukt verschillende aspecten in het tot stand brengen van een spam campagne, zoals de kwaliteit van email-adressen, de effectiviteit van IP-gebaseerde black-lists en de betrouwbaarheid van bots. Dit is mogelijk omdat de auteurs toegang hadden tot een aantal "command en control" servers welke gebruikt werden door het Pushdo/Cutwail botnet. Daarnaast bestudeerden de auteurs Spamdott.biz, een forum gebruikt door de meest notoire spam-gangs, om nieuwe inzichten te verwerven over de underground economy van grootschalige spam campagnes.

* Can we fix the security economics of federated authentication? In deze bijdrage bespreekt Anderson kort vier voorbeelden van federated authenticatie om vervolgens uit te wijden over een veel groter probleem in de toekomst. Als de wereld de visie van Apple, waarin de mobiele telefoon als universeel authenticatie instrument fungeert, accepteert, hoe kan de wereld dit in toom houden? Dit in het bijzonder omdat de telefoon (nog meer) een doelwit zal worden voor kwaadwillenden. Wat gebeurt er als iemand beroofd wordt of als de telefoon geïnfecteerd raakt met malware? Wie moet het slachtoffer bellen en wat moet er gebeuren om het probleem te verhelpen?

Wat was er nog meer in het nieuws =====

* SCADA systemen beschermen op netwerkniveau

Naar aanleiding van de kwetsbaarheden in SCADA waar we vorige week over hebben geschreven, heeft Cisco een technisch advies uitgebracht [1]. Hierin is een overzicht te vinden van maatregelen die te nemen zijn op het gebied van router-, switch- en firewall-configuratie om aanvallers de wind uit de zeilen te nemen.

[1] <http://tools.cisco.com/security/center/viewAlert.x?alertId=22742>

* Kwetsbaarheid in Xerox printers

Xerox heeft afgelopen week aangekondigd dat er een kwetsbaarheid is verholpen in de software van WorkCentre printers [2]. Via een kwetsbaarheid in het Windows filesharing protocol is het voor een aanvaller mogelijk om wijzigingen in het systeem aan te brengen. We hebben hier geen advisory voor uitgebracht, omdat Xerox printers niet voorkomen in een van de deelnemersfoto's. Mocht u toch Xerox printers gebruiken, laat het ons dan weten zodat wij uw foto kunnen aanpassen.

[2] http://www.xerox.com/downloads/usa/en/c/cert_XRX11-002_v1.0.pdf

* 1 April

Ook dit jaar kwamen we weer een groot aantal 1-april grappen tegen. Google kondigde aan dat vanaf 4 april Comic Sans het standaard lettertype voor Google diensten zal worden [3]. Onderzoek heeft aangetoond dat Comic Sans de beste gebruikerservaring biedt. Ook introduceerde Google Translate for Animals voor het Android platform [4]. Na de theepad introduceert Heineken vandaag de Senseo bierpad. Hiervoor is wel een Senseo met hot 'n cold systeem vereist [5]. Bolletje introduceert speciaal beschuit voor linkshandigen [6].

[3] <http://www.google.com/landing/csfe/>

[4] <http://www.google.co.uk/intl/en/landing/translateforanimals/>

[5] <http://www.bierpad.nl/>

[6] <http://www.youtube.com/bolletjetv>

Tot slot wens ik u allen een goed en zonnig weekend toe.

Met vriendelijke groet,


Security specialist

GOVCERT.NL
T +31 70 8887582
I www.govcert.nl
E @govcert.nl

PGP Fingerprint: 

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.

-----BEGIN PGP SIGNATURE-----

ersion: PGP Desktop 10.1.1 (Build 10)
Charset: utf-8

wlcDBQFNldPk9aHKK94RdvsRCFwAAP9gpMzPilcHyqjBg9xrFGZAoXgzHxDuViM8
XtKGr9YeCAD/eIXAAVIs7JGpQUIFtQADiILmwZcO7qI35rJ7zQi2zvE=
=cLmV

-----END PGP SIGNATURE-----

ATT2441893.txt

IB mailing list
IB@lists.govcert.nl

[REDACTED]

Van: [REDACTED]

Verzonden: dinsdag 31 mei 2011 16:08

Aan: [REDACTED]

CC: [REDACTED]

Onderwerp: RE: convocatie AO NV 1 juni

Hoi Mathilda,

Q&A

Er is onderzoek gedaan bij het OT2010 abonnee bestand van Vodafone (ruim 100.000 abonnees). Zoals het zich laat aanzien is het misbruik is zeer beperkt. Minister Donner zal de Kamer over de afloop van het onderzoek informeren. Het verplicht opvolgen van een bepaalde categorie van adviezen van GovCERT wordt nog gezien.

Feitelijke achtergrond (nog niet geschikt voor de Kamer):

Er is onderzocht bij het OT2010 abonnee bestand van Vodafone (ruim 100.000 abonnees) bij hoeveel nummers vanaf 1 december 2010 tot 23 maart jl op afstand de voicemail is beluisterd. In totaal is bij 147 verschillende mobiele nummers op afstand de voicemail beluisterd. Vervolgens is in dit bestand onderzocht of er mobiele nummers van bewindslieden en hoge ambtenaren in voorkwamen. Voor V&J en Defensie is dit geen relevante vraag aangezien zij geen gebruik maken van Vodafone. Van de overige 9 ministeries is van 6 ministeries het resultaat dat 2 mobiele telefoons op afstand zijn beluisterd. De noodzaak van nader onderzoek naar mogelijk misbruik wordt nog gezien. Indien daartoe aanleiding is, wordt onderzocht of de staatsveiligheid in het geding is geweest.

Met vriendelijke groet,

[REDACTED]
senior beleidsmedewerker

Ministerie van BZK

Directoraat Generaal Organisatie en Bedrijfsvoering Rijk

Directie Informatiseringsbeleid Rijk

Schedeldoekshaven 200 | 2511 EZ | Den Haag | H1013

Postbus 20011 | 2500 EA | Den Haag

T (070) 4268581

[REDACTED]@minbzk.nl

<http://www.minbzk.nl>

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

Van: [REDACTED]

Verzonden: dinsdag 31 mei 2011 14:52

Aan: [REDACTED]

Onderwerp: convocatie AO NV 1 juni

Ha [REDACTED]

Hierbij nog de uitnodiging voor het AO Nationale veiligheid morgen waar de cyber security strategie voor is geagendeerd!

gr. [REDACTED]

Ministerie van Veiligheid en Justitie

[REDACTED] Directie Nationale Veiligheid

Schedeldoekshaven 200/Postbus 20011/2500 EA Den Haag

T: [REDACTED] +31 (0) 6 [REDACTED]

[REDACTED]@dgv.minvenj.nl

Ven J-48

[REDACTED]
Van: [REDACTED]
Verzonden: zaterdag 16 juli 2011 16:11
Aan: [REDACTED]
CC: [REDACTED]
Onderwerp: FW: Gebeurtenissen mobiele telefonie in Engeland

Ha [REDACTED]
Meenemen in weekbericht lijkt me.
Groet,
[REDACTED]

-----Original Message-----

From: [REDACTED] (GOVCERT.NL) [mailto:[REDACTED]@govcert.nl]
Sent: Friday, July 15, 2011 03:05 PM W. Europe Standard Time
To: [REDACTED]
Subject: Gebeurtenissen mobiele telefonie in Engeland

Beste Allemaal ,

Zoals je waarschijnlijk hebt gezien spelen in Engeland enkele zaken aangaande het af luisteren van telefonie en voicemails. Omdat deze zaken ook in Nederland veel media-aandacht krijgen deel ik graag onze inzichten hieromtrent met je. Het gaat om twee zaken die onderling geen direct verband hebben:
1. Het af luisteren van voicemails door met name journalisten. 2. Het aanvallen van telefoniesystemen van Vodafone met bij klanten geplaatste apparatuur.

Ad.1

Journalisten hebben op grote schaal voicemails afgeluisterd van onder andere politici en beroemdheden. In essentie gaat het om het inbreken in voicemails, bijvoorbeeld door het raden van (standaard) pincodes en het omkopen van politieagenten en personeel van Vodafone. Deels zijn deze methoden in Nederland ook gebruikt bij het voicemail-incident van enkele maanden geleden. Het is niet uit te sluiten dat deze methodes (opnieuw) ook in Nederland worden gebruikt. In Nederland waarschuwen we onze deelnemers nogmaals voor het goed afschermen van de voicemail. Er zijn (nog) geen aanwijzingen dat gebruik is gemaakt de kraak die onderzoeker Karsten Nohl heeft gepubliceerd voor het kraken van gsm-versleuteling om zo daadwerkelijk telefoongesprekken af te luisteren (waarvoor GOVCERT.NL in 2009 al heeft gewaarschuwd).

Ad. 2

Klanten van Vodafone kunnen in Engeland apparatuur aanschaffen bij Vodafone waarmee thuis het bereik van hun mobiele telefoon verbeterd wordt. Aanvallers zijn in staat geweest met deze apparatuur centrale systemen bij Vodafone aan te vallen waarmee onder andere de (tijdelijke) sleutels van de versleuteling van mobiele telefoons kunnen worden opgehaald. Hiermee kunnen gesprekken worden afgeluisterd. Deze apparatuur wordt nu nog niet in Nederland toegepast. Hier zijn echter wel plannen voor maar er is nog geen introductiedatum. We zullen deze ontwikkelingen in Nederland blijven volgen. De ontwikkeling doet voor Nederland niets af aan het advies om 3G (UMTS) te gebruiken voor mobiele telefonie in plaats van GSM; dat advies blijft daarom gehandhaafd.

Met vriendelijke groet,

[REDACTED]
[REDACTED]

GOVCERT.NL
T +31 70 888 75 55
I www.govcert.nl <<http://www.govcert.nl/>>

██████████@govcert.nl

P.O. Box 96810 2509 JE 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.

Verj-47

Van: [REDACTED] (GOVCERT.NL) [info@govcert.nl]
Verzonden: vrijdag 15 juli 2011 15:44
Aan: info@govcert.nl
Onderwerp: [IB-list] End-of-Week



ATT32839115.bt

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Beste DSC-ers en IB-ers,

De voicemail afluisterpraktijken door diverse media in het Verenigd Koninkrijk toont aan dat kwetsbaarheden in voicemaildiensten van telecomproviders ook werkelijk actief worden misbruikt [1].

Ook in België heeft een journalist, met toestemming van de providers, aangetoond dat het vrij eenvoudig is om voicemails af te luisteren [2].

Al eerder dit jaar is in Nederland veel ophef geweest over het afluisteren van voicemailberichten van derden.

[1] <http://www.bbc.co.uk/news/uk-11195407>

[2] <http://www.humo.be/tws/actua/22871/onze-man-hackte-uw-voice-mails.html>

Welke maatregelen neemt uw organisatie tegen het risico van afluisteren? In maart van dit jaar hebben wij een factsheet gepubliceerd over kwetsbaarheden in voicemaildiensten [3]. Het is aan te raden om, naar aanleiding van de recente berichtgeving, te verifiëren of het advies in het factsheet in uw organisatie is opgevolgd.

[3] <http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-kwetsbaarheden-in-voicemaildiensten.html>

Ieder kwartaal brengt Oracle een Critical Patch update (CPU) uit [4]. Aanstaaende dinsdag worden er door Oracle 78 kwetsbaarheden verholpen in diverse producten.

[4] <http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html>

Verstuurde beveiligingsadviezen

=====

GOVCERT.NL-2010-327 [v1.10][M/M] DLL Insertion kwetsbaarheid in veel

programma's GOVCERT.NL-2011-292 [v1.05][M/M] Mozilla updates verhelpen kwetsbaarheden in Firefox en

Thunderbird GOVCERT.NL-2011-295 [v1.01][L/H] Update voor Asterisk verhelpt kwetsbaarheden GOVCERT.NL-2011-295 [v1.02][L/H] Update voor Asterisk

verhelpt

kwetsbaarheden GOVCERT.NL-2011-305 [v1.02][M/H] Update voor Bind

verhelpt

kwetsbaarheden GOVCERT.NL-2011-305 [v1.03][M/H] Update voor Bind

verhelpt

kwetsbaarheden GOVCERT.NL-2011-310 [v1.00][M/H] Kwetsbaarheden in

Wireshark

Dissectors verholpen GOVCERT.NL-2011-311 [v1.00][M/M] Kwetsbaarheid in

libPNG verholpen GOVCERT.NL-2011-312 [v1.00][L/M] Kwetsbaarheid in OpenOffice verholpen

GOVCERT.NL-2011-313 [v1.00][L/H] Fedora update verhelpt kwetsbaarheden

Microsoft in de kernel GOVCERT.NL-2011-314 [v1.00][M/H] Kwetsbaarheid verholpen in
 Windows Bluetooth stack GOVCERT.NL-2011-315 [v1.00][L/M] Vijftien
 kwetsbaarheden in Windows kernel verholpen GOVCERT.NL-2011-315 [v1.01][L/M] Vijftien kwetsbaarheden
 in Windows kernel verholpen GOVCERT.NL-2011-316 [v1.00][M/M] Diverse kwetsbaarheden
 in Windows Client/Server Runtime Subsystem
 (CSRSS) verholpen GOVCERT.NL-2011-317 [v1.00][M/H] Red Hat update
 kwetsbaarheden in kernel
 GOVCERT.NL-2011-318 [v1.00][L/M] Kwetsbaarheid in RIM BlackBerry
 Enterprise Server verholpen GOVCERT.NL-2011-319 [v1.00][M/H] Trend Micro
 verhelpt kwetsbaarheid in Control Manager GOVCERT.NL-2011-320 [v1.00][M/M] Kwetsbaarheid in
 NetworkManager GOVCERT.NL-2011-321 [v1.00][M/H] Ubuntu update verhelpt kernel
 kwetsbaarheden

Nieuw op de kennisbank (<https://kennisbank.govcert.nl>)

=====

*** PCI DSS Virtualization Guidelines**

De Payment Card Industry (PCI) Security Standards Council heeft een guideline gepubliceerd waarin wordt beschreven wat moet worden gedaan om PCI compliant te zijn in virtuele omgevingen. Het is natuurlijk specifiek geschreven voor organisaties die met betaalkaarten werken, maar de richtlijnen zijn voor iedere organisatie interessant. In deze publicatie worden zowel risico's als aanbevelingen beschreven.

* Guideline for protecting Basic Input Output System firmware ITL Bulletins worden gepubliceerd door het NIST's Information Technology Laboratory en elk bulletin bevat een diepgaande discussie over een specifiek onderwerp. De juni 2011 uitgave gaat over de beveiliging van "Basic Input/Output System (BIOS) firmware".

*** 2011 Mid-Year Security Report**

Blue Coat Systems heeft haar '2011 Mid-Year Web Security Report' gepubliceerd. Voor deze rapportage zijn web-based malware ecosystemen, inclusief de 10 grootste malware distributienetwerken onderzocht.

Wat was er nog meer in het nieuws =====

*** Server Duitse douane gehackt**

Een groep onbekende hackers heeft een server die in beheer was van de Duitse douane gekraakt [5]. Op de server staan onderzoeksgegevens van de politie, namelijk de exacte locatie van verdachten.

[5] <http://www.h-online.com/security/news/item/German-Federal-Police-servers-compromised-1276115.html>

*** Anonymous**

Anonymous heeft de server van FBI-leverancier IRC Federal gehackt en verschillende vertrouwelijke documenten gepubliceerd op Pastebin, waaronder e-mails en VPN inloggegevens [6]. Tevens heeft Anonymous zo'n 90.000 e-mailadressen en wachtwoord hashes van het defensiebedrijf Booz Hamilton gelekt [7].

[6] http://www.security.nl/artikel/37755/1/Anonymous_hackt_FBI-partner_IRC_Federal.html

[7] http://www.security.nl/artikel/3776/1/Anonymous_lekt_90.000_militaire_e-mailaccounts.html

* Britse 3g/umts gesprekken af te luisteren bij Vodafone Hackers hebben privé-antennes, ook bekend als femtocellen, van Vodafone in het Verenigd Koninkrijk gekraakt. Hierdoor kan elk telefoongesprek, dat over het 3g-netwerk wordt gevoerd, worden afgeluisterd.

Wij hebben navraag gedaan bij Vodafone Nederland en zij hebben bevestigd dat de kwetsbaarheid zich

beperkt tot een aantal typen van deze privé-antennes, specifiek voor klanten in de UK.

[8] <http://tweakers.net/nieuws/75604/hackers-kunnen-elk-gesprek-britse-vodafone-klanten-afluisteren.html>

* Artikel over Stuxnet

Ars Technica is de diepte ingegaan met een goed artikel over de Stuxnet saga.

[9] <http://arstechnica.com/tech-policy/news/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history.ars>

Wens ik u tot slot een fijn weekend toe!

Met vriendelijke groet,


security specialist

GOVCERT.NL

T +31 70 888 75 55

I www.govcert.nl

@govcert.nl

PGP Fingerprint: 

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

wlcDBQFOIEQw9aHKK94RdvsRCAfVAP9nh2difAYx6thVEc15EIErWnx36wxHmZHA
Br2eFawY5wD/eqPvKnRtbgBJ9UmEWuzZkVRw6tcYYz3f1v1KNzyzQSQ=
=ofr1

-----END PGP SIGNATURE-----

ATT32839115.txt

IB mailing list
IB@lists.govcert.nl