Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

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

Directie Cyber Security
Beleid

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk
535617

Bijlagen
1

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 10 juli 2014
Onderwerp Antwoorden kamervragen over de kwetsbaarheid van iTunes

Hierbij bied ik u de antwoorden aan op schriftelijke Kamervragen die zijn gesteld door het lid Gesthuizen (SP) over het bericht 'iTunes kwetsbaar voor hackers', waarin wordt bericht dat het muziekprogramma iTunes kampt met een beveiligingsprobleem, waardoor gegevens van gebruikers zouden kunnen worden onderschept. (met kenmerk 2014Z09396 van 22 mei 2014)

De Minister van Veiligheid en Justitie,

I.W. Opstelten

2014Z09396

Directie Cyber Security
Beleid

Datum
10 juli 2014

Ons kenmerk
535617

Antwoorden op vragen van het lid Gesthuizen (SP) aan de minister van Veiligheid en Justitie over de kwetsbaarheid van iTunes (ingezonden 22 mei 2014)

1
Wat is uw reactie op het bericht 'iTunes kwetsbaar voor hackers', waarin wordt belicht dat het muziekprogramma iTunes kampt met een beveiligingsprobleem, waardoor iTunes-wachtwoorden te onderscheppen zijn?[1]

2
Hoe groot acht u de kans dat Nederlandse iTunes- en iCloudgebruikers het slachtoffer zijn of kunnen worden van het beveiligingslek van deze diensten?

3
Zijn er reeds bij u meldingen bekend van personen die het slachtoffer zijn geworden van hackers die misbruik hebben gemaakt van de beveiligingsproblemen van iTunes? Zo ja, om hoeveel Nederlandse gevallen gaat het?

Antwoord 1,2 en 3

Het bericht "iTunes kwetsbaar voor hackers" is mij bekend.

In het door u genoemde geval gaat het om een probleem in de beveiliging van verbindingen van iTunes naar diverse Apple-diensten, waaronder iCloud. Het maken van zo'n verbinding vindt langs beveiligde weg plaats in een gescheiden kanaal ofwel tunnel. Hierbij wordt gebruik gemaakt van het zogeheten TLS/SSL-protocol om deze verbinding op te zetten. Om de verbinding via dit protocol op te zetten wordt gebruik gemaakt van een beveiligingscertificaat. Niet alle varianten van iTunes voor de diverse besturingssystemen controleren deze certificaten op correcte wijze. Hierdoor valt in potentie een aanval uit te voeren door zich in te mengen in het opzetten van de tunnel. Deze lijkt dan veilig, maar is dit niet.

Door het opbouwen van deze onveilige verbinding kunnen gegevens worden onderschept of gemanipuleerd uit verbindingen tussen iTunes en diverse Apple-diensten, waaronder iCloud. Deze gegevens omvatten de gebruikte inloggegevens en bestanden die in iCloud worden opgeslagen of daaruit worden opgehaald.

Op dit moment zijn er bij het Nationaal Cyber Security Centrum geen signalen van actief misbruik van deze kwetsbaarheid in Nederland. Ook de politie heeft blijkens de digitale systemen geen aangiftes/meldingen ontvangen waar uit het verband tussen hacken en iTunes gelegd kan worden.

Door de leverancier in kwestie, Apple, zijn in de afgelopen periode diverse updates uitgevoerd in de kwetsbare variant van de iTunes-software. Hiermee moet naast de nog niet gesignaleerde huidige slachtoffers het aantal toekomstige slachtoffers beperkt geacht worden.

4
Acht u het mogelijk dat, zoals beveiligingsonderzoeker Mark Loman stelt, het beveiligingsprobleem zowel een beginnersfout als een opzettelijke kwetsbaarheid kan zijn? Zo ja, hoe groot is het risico dat het hier een opzettelijke kwetsbaarheid betreft? Zijn er bij u vermoedens dat inlichtingendiensten de kwetsbaarheden gebruiken om communicatie met iCloud te onderscheppen?

5
Kunt u nagaan of eventuele opzettelijke kwetsbaarheden zich ook voordoen bij andere bedrijven, bijvoorbeeld bij Java van Oracle? Kunt u uw antwoord toelichten?

Antwoord op 4 en 5

In deze casus is het aannemelijk dat het beveiligingsprobleem, zoals bovenstaand geschetst, een implementatiefout van de leverancier betreft. Deze implementatiefout op het gebied van het TLS/SSL-protocol is door diverse partijen gemaakt. Ingaan op het vermeende gebruik hiervan door inlichtingen- en veiligheidsdiensten zou daarbij speculatief van aard zijn.

Zoals aangegeven komt een dergelijke implementatiefout vaker voor en betreft het daarbij zeer zeker niet noodzakelijkerwijs een opzettelijke kwetsbaarheid. Ik zie dan ook geen aanleiding om op basis van deze kwetsbaarheid onderzoek te doen naar andere bedrijven. Uiteraard staat het onderwerp van opzettelijk aangebrachte kwetsbaarheden, ook wel backdoors genoemd, zoals reeds in 2012 aangegeven in antwoorden op vragen van de leden Ten Broeke, Hennis-Plasschaert en Verheijen[2] op het netvlies en blijven de inlichtingen- en veiligheidsdiensten alert op alle signalen die veiligheidsrisico's zouden kunnen vormen voor Nederland en haar vitale infrastructuur.

6
Bent u voornemens stappen te ondernemen om de veiligheid van Nederlandse iTunes- en iCloudgebruikers te verbeteren? Zo ja, op welke wijze?

Nee, ik ga geen specifieke stappen ondernemen. Ik vind het wel van belang om de algehele digitale veiligheid, dus niet alleen van iTunes- en iCloudgebruikers, te verhogen. Dit gebeurt middels de in oktober 2013 gepubliceerde tweede Nationale Cyber Security Strategie (NCSS-2).

Bedrijven en instellingen zijn zelf primair verantwoordelijk voor informatiebeveiliging.
In de NCSS-2 is daarnaast aangegeven dat leveranciers een specifieke verantwoordelijkheid (zorgplicht) richting hun klanten hebben en dat security en privacy by design meer dan nu standaard ontwerpbeginselen dienen te zijn.

Tot slot wordt met de NCSS-2 ingezet op een algehele verhoging van de digitale weerbaarheid middels 37 acties. Een belangrijk element daarin is awareness en het hebben van kennis van cybersecurity. Hiertoe zal dit jaar het thema van de jaarlijkse campagne Alert online, van 27 oktober tot 6 november, dan ook kennis van cybersecurity zijn.

Directie Cyber Security
Beleid

Datum
10 juli 2014

Ons kenmerk
535617

1) http://nos.nl/artikel/650363-itunes-kwetsbaar-voor-hackers.html
2) Beantwoording vragen van de leden Ten Broeke, Hennis-Plasschaert en Verheijen over het veiligheidsrisico van Chinese telecomproducenten" d.d. 4 december 2012 en ingezonden met nummer 2012Z17111