



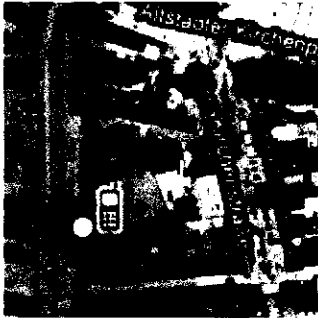
Share on
Facebook

Share on
Twitter

Share via
email

Enter topic to look u

Minister pakt privacyschending politiedatabase aan - Update



Gepubliceerd: Woensdag 23 maart 2011

Auteur: René Schoemaker

Opsporingsdiensten die zich per 1 mei niet houden aan de regels in het opvragen van gegevens van telefoon- en internetgebruikers uit de CIOT database, worden afgesloten.

Minister Opstelten van Veiligheid en Justitie geeft opsporingsdiensten twee maanden de tijd om de procedures op orde te brengen, zodat ze voldoen aan alle regels wat betreft het opvragen van naam, adres en woonplaats van gebruikers van telefonie- en internetdiensten. Anders worden ze afgesloten van het centrale systeem waarmee de gegevens kunnen worden opgevraagd, het zogenaamde CIOT.

Dat schrijft de minister in een brief aan de Tweede Kamer. De minister neemt de maatregel na aanhoudende problemen met procedures, zoals autorisaties en verslagleggingen bij het opvragen van telecomgegevens door opsporingsdiensten. Die kunnen gegevens opvragen als de opsporing dat vereist in het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT).

Al jarenlang een zeef

Volgens Opstelten gelden hiervoor strikte regels als het gaat om het doel van de opvraging, degenen die de gegevens mogen opvragen en de manier waarop vastgelegd moet worden waarom de gegevens zijn opgevraagd. Uit onderzoek van het ministerie blijkt dat een aantal opsporingsdiensten bij herhaling fouten maakt bij die procedures.

Digitale burgerrechtenbeweging Bits of Freedom (BoF) noemt het 'schokkend' dat na jaren audits, verbeterplannen en beloften nog de privacyprocedures nog steeds niet op orde zijn. "Maar nog erger is dat een deel van de opsporingsdiensten die stellen dat ze aan de regels voldoen, in de praktijk deze regels overtreedt," schrijft Ot van Daalen, directeur van BoF, die concludeert dat CIOT "nog steeds zo lek is als een zeef."

Wanneer per 1 mei blijkt dat een opsporingsdienst nog steeds niet voldoet aan de procedures, wordt zij afgesloten van het CIOT-systeem. Wel kan die dienst dan nog gegevens opvragen via een andere dienst die wel aan alle eisen voldoet. "Deze constructie is nodig om te zorgen dat het opsporingsbelang door de maatregel niet in het geding komt", schrijft de minister.

CBP doet ook nog onderzoek

Overigens doet het College Bescherming Persoonsgegevens zelf ook nog onderzoek naar eventuele miststanden in het opvragen van NAW-gegevens. De bevindingen daaruit komen nog, maar voorlopige resultaten sterken de minister in zijn besluit, zo schrijft hij.



Share on
Facebook



Share on
Twitter

Share via
email

Enter topic to look u

De minister is er veel aan gelegen om CIOT op orde te brengen. Want ondanks de problemen heeft Justitie namelijk plannen om het CIOT dramatisch uit te breiden met met toegang tot alle telecomverkeersdata: wie, wanneer, hoelang en waar met wie belt, sms't en mailt. Providers moeten deze gegevens een jaar lang opslaan, sinds de omstreden Wet Bewaarplicht Telecomgegevens vorig jaar werd aangenomen.

Tot nog toe moet Justitie per geval een verzoek indienen aan providers voor deze gegevens. Maar dat is omslachtig, en er worden genante fouten gemaakt, dus moet er directe toegang tot deze immense databanken komen, zodat opsporingsdiensten zelf kunnen spitten.

Update 10.30 uur: kritiek Bits of Freedom toegevoegd.

BIJ DIT ARTIKEL ADVERTEREN?

CBP onderzoekt misbruik opsporingsdatabank CIOT



Gepubliceerd: Vrijdag 24 december 2010

Auteur: Andreas Udo de Haes

Het CBP onderzoekt mogelijke privacyschendingen door opsporings- en inlichtingendiensten bij het opvragen van NAW-gegevens bij telco's. Dat gebeurt 3 miljoen keer per jaar.

Het College Bescherming Persoonsgegevens (CBP) doet diepgravend onderzoek naar ongeoorloofd, onbevoegd en onrechtmatig gespit van politie, Justitie, AIVD en MIVD in de CIOT-databank.

In het CIOT, dat staat voor Centraal Informatiepunt Onderzoek Telecommunicatie, zijn IP-adressen, telefoonnummers en mailadressen gekoppeld aan de NAW-gegevens van Nederlanders.

Het onderzoek van de toezichthouder stond eigenlijk al voor 2009 op de rol, maar is pas sinds enkele maanden ingezet, bevestigt de woordvoester van het CBP.

Onbevoegd en onrechtmatig

De belangrijkste aanleiding is het voortdurende gebrek aan controle over wie, wanneer en hoe in de databank kan grazen. Al jarenlang is de controle op de toegang tot de database beneden de maat, zo bleek uit een audit die eind juli werd gepubliceerd na een beroep op de WOB (wet openbaarheid van bestuur).

Zo kwam tijdens het onderzoek boven water dat opsporingsambtenaren hun inloggegevens uitwisselen, waardoor mensen die niet bevoegd zijn toch de database in kunnen.

Uit een steekproef van enkele tientallen gevallen bleek er weliswaar slechts één opvraging onrechtmatig, maar aangezien er 3 miljoen queries per jaar zijn, is het probleem van wangebruik potentieel groot. Tienduizenden opsporingsambtenaren hebben toegang tot het CIOT, dat elke dag geactualiseerd wordt door de telecomproviders.

Hirsch-Ballin: niet acceptabel

Vaak worden in één zoekactie de NAW-gegevens van honderden abonnees tegelijk opgevraagd. Met dergelijke sleepnetmethoden kan de recherche bijvoorbeeld nagaan wie er ten tijde van een misdaad rond de plaats van het delict aanwezig waren, aan de hand van logfiles gekoppeld aan de locatie van antennes van mobiele telefoonnetwerken.

De publicatie van het audit rapport leidde tot veel ophef en zowel VVD als GroenLinks stelden Kamervragen. In zijn antwoord eind september zegde minister van Justitie Hirsch-Ballin toe de misstanden aan te pakken. "Ik acht dit niet acceptabel," aldus de minister. De bevragingen van het CIOT moeten opnieuw worden getoetst aan de wet- en regelgeving. Waar nodig dient een 'verbeterplan' te komen. Toezicht en controle worden verscherpt en gestandaardiseerd, beloofde Justitie.

Verkeersgegevens ook via CIOT

Ondanks de problemen heeft Justitie echter plannen om het CIOT dramatisch uit te breiden met met toegang tot alle telecomverkeersdata: wie, wanneer, hoelang en waar met wie belt, sms't en mailt. Providers moeten deze gegevens een jaar lang opslaan, sinds de omstreden Wet Bewaarplicht Telecomgegevens vorig jaar werd aangenomen.

Tot nog toe moet Justitie per geval een verzoek indienen aan providers voor deze gegevens. Maar dat is omslachtig, en er worden genante fouten gemaakt, dus moet er directe toegang tot deze immense databanken komen, zodat opsporingsdiensten zelf onbelemmerd kunnen spitten. Een proefballonnetje om ook bankrekeningnummers via het CIOT toegankelijk te maken werd schielijk doorgeprikt.

Onvermijdelijke risico's van misbruik

Ironisch genoeg wees de voorloper van het CBP, de Registratiekamer, er in 1999 bij de voorlopige goedkeuring van het CIOT er al op dat "een te ruim bemeten algemeen informatiebestand onvermijdelijke risico's van oneigenlijk gebruik of zelfs misbruik met zich meebrengt."

Het CBP verwacht het huidige onderzoek naar het CIOT 'in de eerste helft van 2011' af te ronden. Digitale burgerrechtenbeweging Bits of Freedom (BoF) is blij met het onderzoek, dat 'hard nodig' is. "We hopen dat het CBP streng naar deze praktijken kijkt. Het is onacceptabel dat de regering ook nog plannen heeft om het CIOT uit te breiden met verkeersgegevens van internet en telefonie, terwijl keer op keer blijkt dat het in zijn huidige vorm al misgaat", aldus Axel Ambak van BoF.

Relevante whitepaper: Hoe veilig is uw data in de cloud?

[Download](#)

BIJ DIT ARTIKEL ADVERTEREN?