BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KVK 34 12 12 86

M +31 (0)6 39 64 27 38
E rejo.zenger@bof.nl
W www.bof.nl

Ministerie van Veiligheid en Justitie
t.a.v. mevrouw Odinot en mevrouw De Jong

Betreft: aanvulling inbreng evaluatie bewaarplicht

Amsterdam
24 juli 2012

Geachte mevrouw Odinot en mevrouw De Jong,

Bits of Freedom heeft op 21 juni 2012 met u gesproken over de belangrijke evaluatie van de Wet bewaarplicht telecommunicatiegegevens (verder: bewaarplicht). In het gesprek en onze brief hebben we een groot aantal aandachtspunten voor de evaluatie benoemd.

Bits of Freedom wil u, in aanvulling op onze brief, graag wijzen op twee recente voorbeelden uit de praktijk die illustratief zijn voor enkele van de in onze brief genoemde aandachtspunten.

Onbevoegde toegang belgedrag klanten van T-Mobile-dochter Simpel.nl

Door een inbraak op een computersysteem waren vertrouwelijke gegevens van de T-Mobile-dochter Simpel.nl toegankelijk. Onder de gegevens die op deze manier op straat kwamen te liggen, waren ook verkeersgegevens van voor 2011 van klanten van de aanbieder.[1] Hoewel details ontbreken, volgen hieruit wel drie belangrijke constateringen:

1. De opgeslagen verkeersgegevens werden onvoldoende beveiligd. De gegevens stonden in dit geval leesbaar op een met het internet verbonden systeem dat gedeeld werd met andere bedrijven.
2. De gebrekkige beveiliging heeft tot onbevoegde toegang tot zeer persoonlijke gegevens geleid. Grootschalige opslag van gevoelige gegevens vergroot het risico op een datalek.
3. Indien de verkeersgegevens in het kader van de bewaarplicht opgeslagen waren, dan zijn de gegevens niet tijdig verwijderd. De opgeslagen gegevens over het

1 Zie: http://www.nu.nl/internet/2856695/politie-houdt-simpelnl-hacker.html

belgedrag van gebruikers moeten voor de duur van één jaar bewaard worden, waarna zij binnen acht dagen verwijderd moeten zijn. [1]

Gegevens burgers niet veilig bij politie

Uit onderzoek van Bits of Freedom blijkt dat de politie de Wet politiegegevens (Wpg) op grote schaal overtreedt en dat gegevens van burgers niet veilig zijn bij de politie. [2] Dat is relevant voor de evaluatie van de bewaarplicht omdat de bewaarplicht bedoeld is om te garanderen dat opsporings- en inlichtingendiensten over gegevens over het communicatiegedrag van burgers kunnen beschikken.

Uit het onderzoek blijkt dat het diep triest gesteld is met de bescherming van persoonsgegevens bij de politie. Werkelijk geen enkel korps voldoet aan alle wettelijke regels. De Koninklijke Marechaussee leeft minder dan twintig procent van de normen na, en dan nog slechts "op hoofdlijnen". Twaalf korpsen halen voor de helft van de criteria het niveau "voldoet op hoofdlijnen" niet. Slechts drie korpsen scoren op meer dan driekwart van de normen een voldoende.

De problemen doen zich voor over de hele breedte van de wet. De problemen zijn het grootst bij de beveiliging van de persoonsgegevens, het bijhouden van mutaties op autorisaties, het op tijd verwijderen van gegevens die niet langer bewaard mogen worden en de interne controle door het opstellen van een goed jaarverslag.

Grootschalig gevoelige gegevens opslaan is risicovol

Zoals al reeds aangestipt in onze brief zal onderzocht moeten worden of de beveiliging van de gegevens voldoende is, of onbevoegde toegang tot gegevens voorkomen wordt en of de gegevens ook weer tijdig verwijderd worden. Bits of Freedom gaat er vanuit dat u in uw evaluatie ook aandacht zult besteden aan de genoemde praktijkvoorbeelden.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Met vriendelijke groet,

Rejo Zenger

1 Artikel 5, Besluit beveiliging gegevens telecommunicatie
2 Zie: https://www.bof.nl/onderzoek-politie-privacy-audits-2012.pdf