Aanbeveling nr 01/2013 van 21 januari 2013

Betreft: Aanbeveling uit eigen beweging betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken (CO-AR-2013-001)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 30;

Gelet op het verslag van de heer F. Robben, Mevr. D'Hautcourt en de heer E. Gheur;

Brengt op 21 januari 2013 de volgende aanbeveling uit:

I. ONDERWERP VAN DE AANBEVELING

1. Naar aanleiding van een aantal concrete gebeurtenissen[1] die zich recent voordeden en uitgebreid aan bod kwamen in de media, meende de Commissie dat onmiddellijk actie diende te worden ondernomen teneinde een halt toe te roepen aan onbedoelde en ongeoorloofde gegevenslekken, de zogenaamde data breaches, die zoals zij vaststelde doorgaans te wijten zijn aan een onvoldoende gegevensbeveiliging.

2. De technologische evolutie, de koppelingen tussen informatiesystemen, de dematerialisatie van deze systemen en hun dragers en de vermenigvuldiging van digitale informaties vergroten alsmaar het risico op verspreiding van gegevens aan personen die hiertoe geen toegang dienen te hebben.

3. De inadequate beschikbaarheid van "persoonsgegevens" op het internet vormen een ernstig probleem aangezien deze gegevens thans een commerciële waarde kunnen hebben en hun verspreiding oncontroleerbaar wordt indien geen passende veiligheidsmaatregelen worden genomen door elke verantwoordelijke voor een verwerking.

4. Een onvoldoende uitgebouwde informaticastructuur ligt daarbij veelal aan de basis van het probleem en vormt in combinatie met een gebrek aan voldoende ingebouwde controlemiddelen (het vierogenprincipe) en de afwezigheid van een systeem dat tijdig fouten detecteert en rechtzet, de ideale voedingsbodem voor gegevenslekken. Vanuit een permanente bekommernis om dergelijke situaties te voorkomen, formuleert de Commissie dan ook onderstaande aanbevelingen.

II. VEILIGHEIDSMAATREGELEN

2.1 VEILIGHEID VAN DE SYSTEMEN IN HET ALGEMEEN: EVALUATIE VAN DE RISICO'S EN VEILIGHEIDSBELEID

5. De informatiebeveiliging bestaat erin de door een organisatie verwerkte informatie te beschermen voor tal van risico's, hetzij bedreigingen (kwaadwillige interne of externe acties) hetzij kwetsbaarheden (risico's eigen aan de systemen en toepassingen) en laat aldus toe de vertrouwelijkheid, de integriteit alsook de beschikbaarheid van de gegevens te waarborgen.

[1] Publicatie online via Google van de klantenlijst van NMBS Europe op 22 december 2012 dewelke 1.500.000 personen betrof, alsook van een lijst betreffende 500 medewerkers van Defensie op 3 januari 2013 en een gelijkaardige bekendmaking op 8 januari 2013 van de loongegevens van 15.000 personen gebaseerd op een loonenquête uitgevoerd door Jobat.

6. Deze beveiliging moet worden verzekerd door de toepassing van passende maatregelen waaronder organisatorische structuren, regels, processen, procedures maar ook technische systemen.
   Dit geheel van maatregelen moet welbepaald en gedocumenteerd zijn, geïmplementeerd worden, gecontroleerd en zo vaak als nodig verbeterd worden opdat de specifieke doelstellingen inzake veiligheid zouden worden bereikt.

7. De door de Commissie gepubliceerde veiligheidsmaatregelen en de ISO 27.002 norm kunnen in dit opzicht een passend algemeen referentiekader bieden.

8. Bovendien moeten deze maatregelen opgesteld worden in overleg met de rest van de bedrijfsprocessen van de organisatie (de gebruikers van de toepassingen), vertrekkend van de identificatie van de vereisten inzake informatiebeveiliging. Deze vereisten komen voort uit::
   - de systematische evaluatie van de risico's verbonden aan de entiteit en haar gegevensverwerkingen;
   - de toepasselijke wettelijke aspecten;
   - de beroepsprincipes en –vereisten inzake informatieverwerking.

9. De risicoanalyse moet zowel rekening houden met de fysieke veiligheid, de veiligheid op het niveau van het systeem, de veiligheid van de toepassingen, de veiligheid op het niveau van het netwerk en de communicatie (met inbegrip van de veiligheid van opslagsystemen zoals USB…)

10. De invoering van de informatiebeveiliging dient te gebeuren op initiatief, met de steun en onder verantwoordelijkheid van het bedrijfsmanagement maar vergt de deelname van alle bij de informatieverwerking betrokken actoren: informatici, administratieve verantwoordelijken voor de procedures en directieleden.

11. Het veiligheidsbeleid zal voorzien in een voortdurende informatieverstrekking aan de medewerkers van de organisatie over de gelopen risico's in termen van informatieveiligheid alsook over hun wettelijke verplichtingen in het raam van de inzameling, de opslag en de verwerking van persoonsgegevens.

2.2 INFORMATICA-ARCHITECTUUR

12. De informatica-architectuur moet toelaten de beveiliging van de systemen voor informatieverwerking alsook van de beschikbare gegevens te waarborgen, en meer in het bijzonder deze die toegankelijk zijn vanaf het internet.

2.2.1. LOKALE INFORMATICA-ARCHITECTUUR

13. Zij zal gebaseerd zijn op het beginsel van gelaagde beveiliging door implementering van een logische en/of fysieke segmentering van de zones. Rechtstreekse toegang vanaf het internet tot toepassingen zal worden verhinderd via het gelijktijdig gebruik van verschillende middelen naargelang beschikbaarheid, bijvoorbeeld relaisservers zoals "Proxy/Reverse Proxy", door de overdracht van IP-adressen, door een firewall of een behoorlijk geparametriseerde router.

14. In een minimale versie is het onontbeerlijk het lokale netwerk te scheiden van toestellen die toegankelijk zijn vanaf het internet, bijvoorbeeld door het toepassen van firewall/proxy en DMZ. Er moet een systeem worden geïmplementeerd dat een filtering toelaat van de gegevensfluxen tussen deze zones en de alarmsignalen moeten worden opgevolgd en behandeld binnen redelijke termijnen.
    Een optie om het doel te bereiken is evenwel een sterkere structuur te implementeren met ten minste drie "DMZ"-zones, een per niveau:
    - Proxy/Reverse Proxy ;
    - Web applicatie
    - Systeemdatabase die persoonsgegevens bevat

    Andere opties die een volledige scheiding van de fluxen waarborgen zijn mogelijk en dus even aanvaardbaar.

15. Parallel hiermee moet in een systeem worden voorzien dat de analyse en controle toelaat van aanvragen komende van het internet en gericht aan de contentservers teneinde de blootstelling aan kwetsbare punten die ontdekt werden in de toepassingslogica te beperken ("Web Application Firewall"). De meest voorkomende kwetsbaarheden zoals "SQL-injectie" dienen te zijn verbeterd.

16. In functie van de beschikbare middelen, is de invoering en opvolging van een inbraakdetectie (en preventie) –systeem ("IDS/IPS") een pluspunt dat in staat is de abnormale of verdachte activiteiten te ontdekken.

17. Al deze voorzieningen die de veiligheid waarborgen moeten gedocumenteerd worden en de organisatie moet regelmatig veiligheidstest uitvoeren op haar infrastructuur.

2.3 DE VEILIGHEID VAN PERSOONSGEGEVENS

18. De systeemdatabases die persoonsgegevens bevatten mogen slechts toegankelijk zijn vanaf hiervoor bestemde, beveiligde toepassingen en dit des te meer indien vanuit een niet-beveiligde zone toegang kan verkregen worden tot de toepassingen en dus tot deze gegevens.

19. Servers die dergelijke gegevens bevatten mogen niet openbaar toegankelijk zijn op het internet. Indexatie door zoekmotoren zoals Google, Bing, enz. zal worden beperkt tot wat gewettigd is (zie hierna).

20. Uitwisseling van gevoelige of persoonsgegevens met derden zijn slechts toegelaten via beveiligde systemen[2].

21. Ten slotte moeten de extracties van gekwalificeerde/geclassificeerde gegevens uit een productiesysteemdatabase beperkt en gecontroleerd worden.

2.4 ONTWIKKELINGS-/PRODUCTIECYCLUS

22. Er moet worden gezorgd voor een strikte scheiding tussen de ontwikkelings-, test-, aanvaardings-/integratie- en productieomgevingen en de toegang tot de productieomgeving moet beperkt worden tot de behoorlijk gemachtigde en geïdentificeerde systeembeheerders.

23. Om een goede segregatie te verzekeren van functies en toegangen tot informatiesystemen beveelt de Commissie aan:
    - aan de ontwikkelaars de toegang te weigeren tot de toepassingen en de productie-inhoud;
    - procedures in te voeren opdat het in productie nemen van inhoud, toepassingen of zelfs gegevens zou uitgevoerd worden door een hiertoe aangewezen team (Release Management); bij het in productie nemen van zowel statistische als dynamische (applicatie) inhoud, zal een strikte controle moeten uitgeoefend worden op

[2] Zoals de eBox-toepassing die gebruikt wordt voor gegevensuitwisseling tussen de instellingen van de sociale zekerheid

webpagina's en de hieraan gekoppelde online beschikbare bestanden, zelfs en vooral indien deze laatste geen verband houden met een webpagina;

- de gebruikers te betrekken bij de controles alvorens het in productie nemen;
- in functie van de kwalificatie van de gegevens, de toegang te beperken van de databasebeheerders. Er wordt aanbevolen het vierogenprincipe in te voeren voor het beheer en de raadpleging van persoonsgegevens.

2.5 BEHEER VAN INCIDENTEN

24. Het organisme moet beschikken over gekende en gedocumenteerde alarm- en meldingsprocedures ingeval van incidenten die een aantasting betekenen voor de beveiliging van persoonsgegevens. Deze procedures moeten de identificatie- en contactgegevens bevatten van de te contacteren verantwoordelijken op technisch- en managementniveau.

25. Er dient in elke organisatie een duidelijke toewijzing te zijn van de verantwoordelijkheden inzake veiligheid, zowel tijdens de werking als bij incidenten.

26. Meer in het bijzonder moeten in geval van openbaar incident de bevoegde autoriteiten (Privacycommissie) binnen de 48 u geïnformeerd worden over de oorzaken en de schade.

27. Een openbare informatiecampagne zal opgestart worden 24 tot 48u na kennisgeving aan de autoriteiten.

2.6. ONDERAANNEMING (ARTIKEL 16 VAN DE WVP)

28. Wanneer een deel of het geheel van informaticadiensten wordt toevertrouwd aan een onderaannemer, moet de organisatie onder meer waken over de naleving door de onderaannemer(s) van de op de informatieverwerking toepasselijke veiligheidsregels en veiligheidsbeleid, hierbij de rol en verantwoordelijkheden verduidelijkend van iedere interveniënt.

III. JURIDISCH KADER

29. De verplichting voor de verantwoordelijke voor de verwerking om de vereiste technische en organisatorische maatregelen te treffen teneinde de veiligheid van de verwerkte persoonsgegevens te waarborgen, is uitdrukkelijk opgenomen in art. 16, § 4 WVP, genomen in uitvoering van art. 17 van de Europese richtlijn 95/46/EG van 24 oktober 1995

betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, uitdrukkelijk. Ondanks deze verplichting stelt de Commissie echter vast dat in de praktijk hieraan door de verantwoordelijke voor de verwerking in onvoldoende mate aandacht wordt besteed, met de hieraan inherent verbonden en onmiskenbaar nefaste gevolgen voor de persoonsgegevens van de betrokkenen.

30. Hoewel de Commissie reeds het initiatief nam tot publicatie van de "Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens" die als leidraad dient te fungeren voor de verantwoordelijke voor de verwerking bij de implementatie van een degelijk veiligheidsbeleid in uitvoering van art. 16, § 4 van de WVP, brengen de recente gebeurtenissen de Commissie eveneens tot het besluit dat het bestaande reglementair kader dient te worden versterkt, met name door art. 16, § 4 WVP aan te vullen, zodat de Commissie niet alleen de bevoegdheid heeft om aanbevelingen inzake veiligheidsmaatregelen te formuleren, maar deze ook juridisch afdwingbaar te maken. De Commissie zal zich hiertoe richten tot de wetgever.

31. Op het vlak van privacybescherming stelt evenwel niet alleen het gebrek aan veiligheidsgaranties (art. 16, § 4 WVP) een fundamenteel probleem, maar zijn ook de art. 4, § 1, 2° WVP en 9 WVP in het geding.

32. Art. 4, § 1, 2° WVP laat niet toe dat gegevens waarover een verantwoordelijke voor de verwerking beschikt, worden hergebruikt voor een doeleinde dat onverenigbaar is met het doeleinde waarvoor hij deze gegevens initieel heeft verkregen. Het spreekt voor zich dat de online publicatie van gegevens die hiervoor oorspronkelijk niet bestemd waren, een gegevensverwerking uitmaakt die een inbreuk inhoudt op dit voorschrift, dewelke bovendien strafrechtelijk wordt gesanctioneerd door art. 39, 1° WVP.

33. In deze context dient ook art. 9 WVP onder de aandacht te worden gebracht. Deze bepaling legt de verantwoordelijke voor de verwerking de verplichting op om de betrokkenen te informeren over de doeleinden waarvoor de gegevens zullen worden aangewend. Indien later blijkt dat de verantwoordelijke de gegevens heeft gebruikt voor een doeleinde dat onverenigbaar is met het oorspronkelijke doeleinde en waaromtrent hij geen informatie verschafte aan de betrokkenen, dan begaat hij een inbreuk die strafbaar is op grond van art. 39, 4° WVP.

34. Gelet op het onmiskenbare belang om in de nodige waarborgen inzake gegevensbescherming te voorzien, dringt de Commissie er dan ook bij de

verantwoordelijken voor de gegevensverwerking op aan de onderstaande aanbevelingen inzake veiligheidsmaatregelen (punt II.) nauwgezet te respecteren. Meer nog, in geval van niet-naleving ervan engageert de Commissie zich ertoe om alle wettelijk beschikbare middelen in te zetten waardoor de aansprakelijkheid van de verantwoordelijke voor de verwerking in het gedrang komt en deze het risico loopt te worden vervolgd. Immers, tenzij de wet anders bepaalt, doet de Commissie bij de procureur des Konings aangifte van de misdrijven waarvan zij kennis heeft (art. 32, §2 WVP).

35. Dit geheel van regels vormt dus de door iedere verantwoordelijke voor een verwerking na te leven regels van de kunst teneinde een optimale informatieveiligheid te verzekeren en bijgevolg de beveiliging van de persoonsgegevens van de betrokkenen te waarborgen.

36. De onderhavige aanbeveling zal de gerechtelijke autoriteiten, wanneer aanklachten bij hen aanhangig worden gemaakt of zij deze ambtshalve in behandeling nemen, toelaten ieder feit dat een inbreuk vormt op de WVP te beoordelen alsook de ernst ervan te evalueren.

37. Ten slotte herinnert de Commissie er aan dat de verantwoordelijke voor de verwerking verantwoordelijk is voor de schade die voortvloeit uit een handeling die in strijd is met de bij of krachtens de WVP bepaalde voorschriften.
Hij is van deze aansprakelijkheid ontheven indien hij bewijst dat het feit dat de schade heeft veroorzaakt hem niet kan worden toegerekend (art. 15*bis* van de WVP).

OM DEZE REDENEN

beveelt de Commissie aan

dat elke verantwoordelijke voor de verwerking de bovenstaande aanbevelingen nauwgezet naleeft en toepast volgens de regels van de kunst, zodat hij een veiligheidsbeleid hanteert waardoor hij beantwoordt aan de norm van de goede huisvader.

De Wnd. Administrateur, De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere