Advies 62/2016 van 23 novembre 2016

Betreft: Adviesaanvraag van het Centrum voor Cybersecurity België over het project « Botnet Eradication » (CO-A-2016-065)

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 29;

Gelet op de adviesaanvraag van het Centrum voor Cybersecurity België, ontvangen op 3 oktober 2016;

Gelet op het verslag van de heer Frank De Smet;

Brengt op 23 november 2016 het volgend advies uit:

De Commissie vestigt er de aandacht op dat er recent nieuwe Europese regelgeving inzake de bescherming persoonsgegevens uitgevaardigd werd: betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens Deze akten verschenen in het Europese Publicatieblad van 4 mei 2016[1].

De verordening, meestal GDPR (general data protection regulation) of AVG (Algemene verordening gegevensbescherming) genaamd, is twintig dagen na publicatie of op 24 mei 2016 van kracht en wordt, twee jaar later automatisch van toepassing, zijnde op 25 mei 2018. De richtlijn voor politie en justitie moet via nationale wetgeving omgezet worden tegen uiterlijk 6 mei 2018.

Voor de Verordening betekent dit dat vanaf 24 mei 2016, gedurende de uitvoeringstermijn van twee jaar, op de lidstaten enerzijds een positieve verplichting rust om alle nodige uitvoeringsbepalingen te nemen en anderzijds ook een negatieve verplichting, de zogenaamde “onthoudingsplicht”. Laatstgenoemde verplichting houdt in dat er geen nationale wetgeving mag worden uitgevaardigd die het door de Verordening beoogde resultaat ernstig in gevaar zou brengen. Ook voor de Richtlijn gelden gelijkaardige principes.

Het verdient dan ook aanbeveling om desgevallend nu reeds op deze akten te anticiperen. Het behoort in de eerste plaats aan de adviesaanvrager(s) toe om hiermee rekening te houden in zijn (hun) voorstellen of ontwerpen. De Commissie heeft in onderhavig advies, in de mate van het mogelijke en onder voorbehoud van mogelijke bijkomende toekomstige standpunten, alvast gewaakt over de hoger geschetste negatieve verplichting.

---

[1]Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

I. VOORWERP EN CONTEXT VAN DE AANVRAAG

1. Het Centrum voor Cybersecurity België (hierna "CCB" of "de aanvrager") heeft het advies van de Commissie gevraagd over het voorstel van beleidsnota « Botnet Eradication » die rekening wenst te houden met de potentiële problemen die deze nota zou kunnen impliceren inzake privacy.

2. Een botnet is een netwerk van besmette systemen (ook "zombies" genoemd) waarvan diegene die er de controle over heeft (of de "botnet herder") gebruik kan maken voor kwaadaardige doelstellingen zoals het versturen van spamberichten, DDOS[2] aanvallen enz. Hiertoe zal de bornetherder in het algemeen gebruik maken van een tussenschakel in de vorm van een « command and control » server om zijn opdrachten door te sturen naar het netwerk van besmette systemen zodat deze andere systemen kunnen aanvallen en informatie stelen, maar waardoor deze zelf moeilijker te traceren is.

3. Momenteel ontvangen de Belgische openbare diensten inlichtingen over besmette systemen van bronnen zoals Microsoft, Shadowserver[3] of CERT[4] (cybersecurity teams ("brandweer van het internet") die men overal ter wereld vindt), doch deze inlichtingen worden op dit moment niet geëxploiteerd, voornamelijk door het feit dat er geen wettelijk kader bestaat voor de samenwerking tussen de Belgische openbare diensten en de telecomoperatoren (hierna "ISP's"). Dit heeft als gevolg dat de eindgebruikers, de voornaamste betrokkenen bij deze inlichtingen, niet geïnformeerd worden en bijgevolg waarschijnlijk niet weten dat hun systemen besmet zijn. De aanvrager stelt dat het in België gaat om honderdduizenden besmette systemen.

4. Bijgevolg bestaat het doel van het door de aanvrager gevoerde beleid erin de voorkeur te geven aan een benadering waarbij de eigenaars (zowel natuurlijke als rechtspersonen) van besmette systemen verwittigd worden over het vastgestelde probleem en geïnformeerd worden over de oplossingen die kunnen toegepast worden om hun systeem te ontsmetten.

5. Het ter advies aan de Commissie voorgelegde document bevat dus een werkwijze die de aanvrager wenst te zien toepassen tussen de verschillende partners.

---

[2] Distributed denial of service attack, met als doel een dienst uit te schakelen

[3] Shadowserver is een in 2014 opgerichte stichting samengesteld uit vrijwilligers uit de professionele beveiliging wereldwijd die zich inzetten in de strijd tegen de internetcriminaliteit. Voor meer informatie zie volgende pagina: https://www.shadowserver.org/wiki.

[4] Computer emergency response teams.

6. Aangezien de aanvrager bekommerd is om het vrijwaren van het privéleven van de betrokkenen heeft hij ervoor geopteerd de Commissie te betrekken bij de voorbereidende discussies voorafgaand aan de opmaak van deze tekst.

7. De Vereniging van Internet Service Providers in België (hierna « ISPA ») werd eveneens betrokken bij het project samen met het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT), opdat het grootste aantal eindgebruikers zou kunnen worden bereikt. De samenwerking tussen het BIPT en ISPA is immers essentieel om de ISP's die geen lid zijn van de ISPA bij het project te betrekken. De aanvrager verduidelijkt eveneens dat het BIPT een advies zal uitbrengen over de punten die verband houden met de wet van 13 juni 2005 *betreffende de elektronische communicatie*.

II. ONDERZOEK TEN GRONDE

8. De aan de Commissie voorgelegde tekst is een voorstel van beleidsnota. De Commissie vestigt de aandacht van de aanvrager hierop en herinnert eraan dat hij niet geacht wordt zich uit te spreken over de opportuniteit van een te volgen beleid maar beschouwt het initiatief van de aanvrager om haar te raadplegen over de privacy-issues, als positief.

A. Finaliteit

9. Het voorstel strekt ertoe een werkwijze in te voeren tussen de verschillende partners en betrokkenen om efficiënt de strijd aan te gaan tegen botnets met het oog op hun uitroeiing. De beoogde procedure moet het mogelijk maken dat de betrokkenen die getroffen zijn door een besmet systeem, rechtstreeks geïnformeerd worden door de ISP's. Deze laatsten zullen aan hun klanten eveneens de nodige informatie moeten verstrekken over de te ondernemen stappen om hun systeem te "ontsmetten". De aanvrager verduidelijkte dat de procedure enkel gelanceerd wordt voor besmettingen van pc's, tablets en smartphones. Besmettingen van toestellen in het raam van het Internet der dingen (Internet of things) behoren niet tot het toepassingsgebied van dit initiatief.

10. De Commissie is van mening dat het beoogde doeleinde welbepaald, uitdrukkelijk omschreven en gerechtvaardigd is zoals bedoeld in artikel 4, § 1, 2° van de Privacywet maar stelt zich toch vragen bij de doeltreffendheid van de door de aanvrager geplande maatregelen. De Commissie meent immers dat de auteurs van aanvallen met behulp van botnets op technisch gebied zeer snel zullen reageren zodat de voorgestelde maatregelen mogelijk niet echt effectief zullen zijn. Hierdoor zou heel het opzet kunnen neerkomen op symptoombestrijding

op korte termijn. De Commissie heeft ook vragen bij de verantwoordelijkheid die teveel wordt gelegd bij de eindgebruikers van wie de computers besmet zijn, terwijl de rol van de ISP's wordt beperkt tot het sturen van berichten naar de betrokken klanten zonder verdere structurele maatregelen. De Commissie acht het dus belangrijk dat deze laatsten een actievere rol dienen op te nemen door hun klanten bij te staan om hun systemen te vrijwaren van malware en er voor te zorgen dat alle mogelijke maatregelen worden genomen teneinde de impact van een actieve aanval te minimaliseren. In elk geval meent de Commissie dat het rechtstreeks contact opnemen met de betrokkenen, zoals bepaald in het ontwerp, dient te worden aangemoedigd maar dit mag dus geen maatregel zijn die op zichzelf staat.

B. Rechtmatigheid en proportionaliteit van de beoogde verwerking

11. De Commissie herinnert eraan dat een IP-adres, voor zover het toelaat een persoon te identificeren, moet beschouwd worden als een persoonsgegeven.

12. Concreet stelt de aanvrager de volgende procedure voor:

1° meerdere openbare diensten (volgens verduidelijking door de aanvrager CERT.be, CCB, politie en gerecht) ontvangen lijsten met de IP-adressen (samen met timestamps[5] en poortnummers[6]) van de besmette systemen;
2° deze informatie wordt doorgestuurd aan het federale cyber emergency team (het noodinterventieteam inzake informaticaveiligheid - CERT.be), dat op beveiligde wijze instaat voor het centraal beheer van deze lijsten;
3° CERT.be staat in voor het globaal beheer van deze lijsten, met name voor het samenvoegen, rangschikken en filteren ervan. De bron en de betrouwbaarheid van deze lijsten wordt gecontroleerd. Vervolgens worden de lijsten opgesplitst per provider (ISP) via de openbare gegevens zoals DNS[7], whois[8] (laten toe om kenmerken – zoals de ISP - van een IP-adres of domeinnaam te achterhalen, zie bv. http://whois.domaintools.com) enz. Er gebeurt in dit stadium geen identificatie van de eigenaars van de geïnfecteerde systemen. CERT.be neemt ook contact op met de politie om zich ervan te verzekeren eventueel door hen gevoerd onderzoek niet wordt geschaad door de initiatieven van CERT.be.
4° CERT.be stuurt de opgesplitste lijsten naar de betrokken providers die deelnemen aan het project. De lijsten bevatten de besmette IP-adressen, de « timestamp » en de poortnummers,

[5] Tijdstempel met de datum en het uur waarop een informaticaverrichting werd uitgevoerd.
[6] Dit cijfer wijst op de toepassing waarvoor de gegevens zijn bestemd.
[7] Het systeem van domeinnamen.
[8] Protocol dat toelaat de registers te raadplegen met de geregistreerde gebruikers van domeinnamen of IP-adressen.

alsook eventueel specifieke informatie voor de providers (de aanvrager verduidelijkt dat deze specifieke informatie gaat over de aard van de malware en hoe deze kan worden verwijderd;
5° De ISP stuurt een bericht naar zijn klant en kan eventueel andere maatregelen nemen;
6° De eindgebruiker wordt aangemoedigd om zijn systeem te ontsmetten. Bovendien zullen het CCB en/of CERT.be een portaalsite creëren met informatie die de eindgebruiker moet helpen en bijstaan om het systeem te ontsmetten. Indien hij hier niet in slaagt zal hij doorverwezen worden naar een specialist (via het bericht dat hem zal worden gestuurd of via de portaalsite).

13. De Commissie merkt op dat de beoogde procedure de interventie impliceert van verschillende actoren. In een eerste fase krijgen private of openbare entiteiten (omdat hun systemen worden aangevallen en waardoor zij de IP-adressen kunnen achterhalen van de (Belgische) aanvallers) zoals Microsoft, Shadowserver of de CERTs, andere dan CERT.be, kennis van besmette IP-adressen op Belgisch grondgebied en sturen vervolgens de lijsten met deze IP-adressen door aan de Belgische openbare diensten (CCB, politie en justitie) of aan CERT.be.

14. De Commissie merkt op dat de huidige omschrijving van de opdracht van CERT.be enkel betrekking heeft op Belgische ondernemingen en (gouvernementele) organisaties. Aangezien CERT.be door dit project geacht wordt de IP-adressen te verwerken die met name verbonden zijn met natuurlijke personen, zou deze opdracht in die zin opnieuw moeten worden gepreciseerd. Temeer daar er een portaalsite met voor natuurlijke personen bestemde informatie zal worden opgericht in het kader van het project.

15. De aanvrager verduidelijkte overigens aan de Commissie dat met betrekking tot de aftoetsing die gebeurt bij de politie, deze niet zal bestaan uit de mededeling van IP-adressen of andere persoonsgegevens aan de politie, maar dat het belangrijk is - alvorens de procedure bij de ISP's op te starten - dat het CERT.be zich ervan vergewist dat het een eventueel lopend onderzoek bij de politie in het kader van een welbepaald type malware hierdoor niet in het gedrang brengt. CERT.be deelt enkel de naam van een botnet waarvoor er een procedure zal worden opgestart aan de politie mee. De Commissie neemt hiervan akte.

16. De Commissie herinnert eraan dat opdat de geplande verwerking conform zou zijn aan artikel 4, § 1, 1° en 3° van de WVP, de verwerkte gegevens ter zake dienend en niet overmatig moeten zijn in het licht van de doeleinden waarvoor zij werden verkregen en verder worden verwerkt, en dus beperkt dienen te worden tot wat voor de verwerkingsverantwoordelijke noodzakelijk is om dit doeleinde te verwezenlijken.

17. Betreffende de procedure om via de ISP's de betrokkenen te informeren over een mogelijke besmetting, meent de Commissie dat het inderdaad gaat om de minst intrusieve wijze om dit te doen. De betrokkenen zijn immers contractueel verbonden met hun provider die reeds over voldoende persoonsgegevens beschikt om met hen in contact te treden.

18. In elk geval blijkt dat de strijd tegen botnets en elke andere vorm van gerichte aanvallen via informaticasystemen een opdracht van openbaar belang is in het licht van de grote veiligheidsproblemen die gepaard gaan met het gebruik van deze botnets en dat de informatieverstrekking aan de betrokkenen primordiaal is om de strijd doeltreffend te kunnen voeren.

19. In dit opzicht zijn de door de aanvrager geplande gegevensverwerkingen toelaatbaar gelet op artikel 5, e) van de WVP aangezien zij noodzakelijk zijn voor de voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, door de aanvrager en de ISP's. Wat deze laatsten betreft, bepaalt artikel 114, § 1 van de wet van 13 juni 2005 betreffende de elektronische communicatie immers het volgende: "*Ondernemingen die openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten aanbieden, treffen de passende technische en organisatorische maatregelen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen, eventueel samen wat de veiligheid van het netwerk betreft*". In dit verband stelde het BIPT in een brief aan de aanvrager dat het project van de CCB verenigbaar is met artikel 114, § 1 van de wet van 13 juni 2005 *betreffende de elektronische communicatie,* aangezien de botnets opstopping kunnen veroorzaken en de continuïteit van de netwerken in het gedrang kunnen brengen alsook de elektronische communicatiediensten die op basis ervan worden geleverd.

20. Etappe 5 van de procedure (cf. supra punt 12) impliceert dat de ISP zijn klant identificeert aan de hand van het IP-adres. Volgens artikel 124 van de voormelde wet betreffende de elektronische communicatie is deze identificatie in principe niet toegelaten[9] maar volgens artikel 125, § 1, 2° van diezelfde wet is dit verbod niet van toepassing "*wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische-communicatiedienst te garanderen".* De Commissie noteert bijgevolg dat de identificatie van de klant door de ISP in het raam van onderhavige adviesaanvraag wel degelijk gewettigd is.

[9] Indien men daartoe geen toestemming heeft gekregen van alle andere, direct of indirect betrokken personen, mag niemand met opzet de personen identificeren die bij de overzending van de informatie en de inhoud ervan betrokken zijn.

C. Verantwoordelijkheid voor de verwerking

21. De Commissie onderkent vier niveaus van verwerkingsverantwoordelijken: de entiteiten die worden aangevallen en informatie verzamelen over hun belagers, de openbare diensten die verslagen ontvangen over de botnets, CERT.be en de ISP's.

22. De huidige beleidsnota is niet expliciet in dit verband. De Commissie verzoekt de aanvrager om deze verschillende verwerkingsverantwoordelijken hierin duidelijk te identificeren.

D. Veiligheid van de geplande verwerking

23. Overeenkomstig artikel 16 van de WVP dienen de verwerkingsverantwoordelijken de nodige technische en organisatorische maatregelen te nemen om de persoonsgegevens te beschermen. Deze informatiebeveiliging moet worden verzekerd door de toepassing van passende maatregelen[10], waaronder organisatorische structuren, regels, processen en procedures maar ook technische systemen. Dit geheel van maatregelen moet worden vastgelegd en gedocumenteerd, uitgevoerd, gecontroleerd en zo vaak mogelijk worden verbeterd opdat de specifieke doeleinden inzake veiligheid worden bereikt. De Commissie onderstreept onder meer dat elke verwerkingsverantwoordelijke zal moeten bepalen welke personen en/of functie binnen zijn organisme, recht hebben op toegang tot de persoonsgegevens (strikt gebruikers- en toegangsbeheer voor toegang tot de lijsten met geïnfecteerde systemen). Indien bovendien een beroep wordt gedaan op een verwerker dienen de ad hoc bepalingen van artikel 16 van de WVP strikt in acht te worden genomen. De aanvrager verduidelijkte ook dat het aantal personen dat toegang zal hebben tot de lijsten sowieso zal beperkt worden tot het strikte minimum. Zo zullen bv. op het niveau van de ISP's de medewerkers van de klantendiensten geen toegang hebben tot deze lijsten.

E. Bewaringstermijn

24. De aanvrager verduidelijkte aan de Commissie dat hij wenste dat de ISP's alsook het CERT.be de gegevens (lijsten met gegevens over geïnfecteerde systemen) gedurende 6 maanden zouden mogen bewaren, wat volgens hem een redelijke termijn is om enerzijds de informatie over de besmetting te verwerken en anderzijds te vermijden dat een internetgebruiker meermaals wordt gecontacteerd voor eenzelfde alarm. Na de periode van zes maanden zullen de gegevens worden vernietigd.

[10] Zie de door de Commissie gepubliceerde veiligheidsmaatregelen, https://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens_0.pdf

25. In het licht van het nagestreefde doeleinde, met name het versturen van een waarschuwing aan de personen die getroffen zijn door een besmetting van hun systeem, meent het Comité dat deze termijn niet gerechtvaardigd is. De Commissie verduidelijkt dat zij geen enkele informatie ontving met betrekking tot de bewaringstermijnen van de andere verwerkingsverantwoordelijken (openbare diensten en entiteiten die worden aangevallen en gegevens inzamelen over hun belagers). Om conform artikel 4, §1, 5° van de WVP te zijn dient de bewaringstermijn proportioneel te zijn aan het beoogde doeleinde. De Commissie verzoekt de aanvrager om de bewaringstermijn te herzien.

F. Informatieverstrekking aan de betrokkenen

26. De aanvrager verduidelijkt in zijn voorstel dat de boodschap die door de ISP's aan de betrokken eindgebruikers zal gericht worden een informatief en preventief karakter zal hebben, duidelijk zal moeten zijn en volgende inlichtingen bevatten:
    - Duidelijke informatie over het project en zijn context (met logo's ISP en CCB/CERT.be);
    - Een waarschuwing met betrekking tot een mogelijke besmetting;
    - De potentiële impact van deze besmetting, zowel voor de betrokkenen als voor de andere potentiële slachtoffers indien hun systeem zou gemobiliseerd worden voor een cyberaanval;
    - Informatie over de wijze waarop de gebruiker zijn systeem kan herstellen en over de manier om besmetting in de toekomst te vermijden;
    - Een verwijzing naar de portaalsite en in voorkomend geval naar een specialist indien nodig.

27. De aanvrager voorziet de oprichting van een portaalsite « safeonweb.be », voor de informatieverstrekking aan de eindgebruikers (informatie over hoe een systeeminfectie kan worden opgelost en vermeden worden in de toekomst).

28. De aanvrager vermeldt eveneens de mogelijkheid om te voorzien in een contactpunt om de eindgebruiker toe te laten vragen te stellen over zijn specifieke situatie in het kader van een systeembesmetting. De aanvrager heeft verduidelijkt dat er noch bij dit contactpunt van de CCB/CERT.be noch bij de klantendiensten van de ISP's een bijkomende verwerking van persoonsgegevens zal plaatsvinden in het kader van een contactopname door de betrokkenen (er zal in dit kader geen bijkomende registratie gebeuren van gegevens op persoonsniveau). Enkel algemene gegevens zouden worden geregistreerd (bv. aantal contactopnames). De periodieke rapportage betreffende de reacties van de eindgebruikers in Punt 8 van de

beleidsnota heeft dus geen verdere verwerking van persoonsgegevens tot gevolg volgens bijkomende informatie gegeven door de aanvrager.

29. De Commissie dringt er bij de aanvrager op aan dat de boodschap die zal gericht worden aan de eindgebruiker die getroffen is door een besmetting, zo duidelijk en volledig mogelijk zou zijn. Zowel wat de besmetting zelf betreft als de middelen om deze te verhelpen. In ieder geval moet de informatie zoals beschreven in artikel 9 van de WVP worden verstrekt. De commissie stelt voor om de informatie naar de eindgebruiker wat de hem betreffende gegevens aangaat, nog aan te vullen met de volgende punten:

    - Verwijzing naar het contactpunt en de wijze om dit te contacteren alsook de eventuele mogelijkheid om de klantendienst van zijn ISP te bellen;
    - Details over de specifieke besmetting (en remediëring) waarvan hij slachtoffer is;
    - Het bestaan van een recht op toegang en verbetering;
    - De ontvangers of categorieën ontvangers van de gegevens;
    - De expliciete vermelding van de doeleinden en de verantwoordelijken voor de verwerking;
    - De oorsprong van de informatie over de specifieke besmetting van het systeem van de eindgebruiker;
    - De mogelijke juridische gevolgen bij het negeren van de boodschap.

30. Aangaande dit laatste punt met betrekking tot de mogelijke juridische gevolgen die ten laste van de eindgebruiker zouden worden gelegd, formuleert de Commissie ernstige twijfels bij de rechtmatigheid en de uitvoerbaarheid hiervan. In elk geval is het zeer belangrijk zich ervan te vergewissen dat de eindgebruiker volledig en duidelijk werd geïnformeerd over alle mogelijke gevolgen, met inbegrip van deze ingevolge het negeren van de waarschuwingsboodschap.

31. De Commissie wenst de aanvrager er attent op te maken dat de mogelijkheid bestaat dat dergelijke boodschappen door kwaadwilligen worden hergebruikt (na manipulatie van de originele boodschap, waarbij er dan bijvoorbeeld wordt doorverwezen naar websites waar men gevoelige informatie tracht te bekomen of waar er juist malware wordt geïnstalleerd, maar waarbij de eindgebruiker denkt dat het gaat over een authentieke boodschap van de ISP) voor o.a. phishing doeleinden. Het resultaat hiervan (toename van het aantal besmette systemen) zou dan tegengesteld zijn aan hetgene dat men juist wil bereiken met het onderhavig project. De Commissie vraagt daarom aan de aanvrager om de nodige voorzorgen te nemen zodat de boodschap aan de eindgebruikers bijkomende elementen bevat die aangeven dat de boodschap wel degelijk van zijn ISP komt (het logo van een ISP of CCB/CERT.be is op zich allerminst een garantie dat het bericht authentiek is). Deze bijkomende elementen kunnen er bijvoorbeeld in bestaan om informatie op te nemen in de

boodschap waarvan kan verondersteld dat deze normaal gezien alleen kan afkomstig zijn van de ISP (zoals bijvoorbeeld het klantnummer of zelfs een digitale handtekening - het versturen van een boodschap met een link die de betrokkene doorverwijst naar een gecertificeerde website (waar dan de eigenlijke boodschap staat) kan in dit kader ook een oplossing zijn). Ook zou men er voor kunnen kiezen om de boodschap alleen op papier te verzenden met de reguliere post. De Commissie onderkent echter de bijkomende kosten die deze laatste oplossing met zich meebrengt.

32. Bovendien zou het ook nuttig zijn om aan de eindgebruiker en in de boodschap zelf tips te geven waardoor hij kan controleren dat de weblinks die in de boodschap zijn opgenomen wel degelijk verwijzen naar te vertrouwen websites (bij hergebruik door kwaadwilligen zullen deze tips dan ook moeten worden aangepast, wat veel meer opvalt dan enkel manipulatie van onderliggende links). Tenslotte kan in de boodschap ook aangegeven worden dat er op geen enkele manier gevoelige informatie zal worden opgevraagd.

33. De Commissie vestigt er de aandacht op dat de persoonsgegevens die in het kader van deze adviesaanvraag worden gebruikt, niet verder mogen worden verwerkt voor direct marketing doeleinden (bv. het opzetten van mailings door de ISP specifiek naar de betrokkenen met een besmet systeem om de eigen commerciële anti-malwaretools aan te prijzen) tenzij de betrokkene hierover vooraf werd ingelicht en de mogelijkheid kreeg zich te verzetten tegen deze verwerking.

34. De verstrekte informatie moet eveneens duidelijk vermelden wie de verwerkingsverantwoordelijke is bij wie de betrokkene in voorkomend geval zijn rechten op toegang, verbetering en verzet kan laten gelden.

OM DEZE REDENEN,

de Commissie brengt, onder voorbehoud van de inachtneming van de in onderhavig advies geformuleerde opmerkingen, een gunstig advies uit over het voorstel van beleidsnota van het Centrum voor Cybersecurity België in het raam van de uitroeiing van botnets.

De Administrateur f.f., De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere