Bachelorscriptie

Radboud Universiteit

Een technische en juridische analyse van het protocol van de *Veilige E-mail Coalitie*

Auteur:
Marvin van Bekkum
s4341619

Eerste begeleider/beoordelaar:
prof. dr. B.P.F. (Bart) Jacobs
b.jacobs@cs.ru.nl

Tweede begeleider/beoordelaar:
mr. J.A. (Janita) Hofman
j.hofman@jur.ru.nl

22 augustus 2017

Woord vooraf

Ik wil mijn scriptiebegeleiders bedanken voor hun toewijding tijdens het werken aan deze scriptie. Ik bedank bovendien mijn hoofdbegeleider prof. Jacobs voor het bedenken van een geschikt onderwerp om deze scriptie over te schrijven.

Samenvatting

Een tijd geleden beschreef Forum Standaardisatie, een Nederlands overheidsorgaan, op een website het plan om een nieuw protocol tegen afluisteren en phishing (hierna: "het protocol") te introduceren in samenwerking met diverse (private) bedrijven. Dat plan is het resultaat van een publiek-privaat samenwerkingsverband genaamd de *Veilige E-mail Coalitie* (hieronder: "de Coalitie").

Vanaf mei 2018 is een nieuwe gegevensbeschermingsverordening van kracht, de Algemene verordening gegevensbescherming (hierna: "de Verordening"). De consequenties van de invoering van de Verordening zijn tot dusver onduidelijk. Daarom wordt in deze scriptie de volgende vraag behandeld: *welke voor de Coalitie relevante plichten vloeien voort uit de bepalingen van de Algemene verordening gegevensbescherming, en in hoeverre voldoen de partijen in de Coalitie aan die plichten door het protocol te implementeren?*

Uit het antwoord op de in de vorige alinea uitgewerkte vraag blijkt dat de eindgebruiker door het protocol onvoldoende wordt beschermd tegen een aantal risico's. Het protocol beschermt bijvoorbeeld niet goed genoeg tegen het risico dat e-mails massaal kunnen uitlekken. Dat die risico's bestaan blijkt na een onderzoek naar welke van de securitydoelen Confidentiality, Integrity en Authentication het protocol bereikt.

Op het moment niet-bestaande jurisprudentie over de Verordening zou nodig zijn om de in de vorige alinea beschreven vraag buiten elke redelijke twijfel te kunnen beantwoorden. Echter, door enkel het protocol te implementeren worden geen maatregelen genomen om de in de vorige alinea beschreven risico's te bestrijden. Daarom is volgens de auteur niet voldaan aan plichten uit de Verordening.

Deze scriptie bespreekt vier mogelijke manieren om de bovengenoemde risico's te bestrijden. De combinatie van invoering van directe versleuteling tussen serviceproviders van e-mail, en versleuteling tussen die serviceprovider en hun eindgebruikers wordt daaruit gekozen als suggestie. Het doel van die suggestie is het bestrijden van de risico's waarvan hierboven sprake was.

Lijst van figuren

3.1 Een mogelijk SMTP-sessie tussen Alice (verzender) en Bob (ontvanger). 11
3.2 Een voorbeeld van het uitwisselen van berichten middels asymmetrische versleuteling. 12
3.3 Een voorbeeld van het opzoeken van een IP-adres dat bij een bepaalde domeinnaam hoort. 13
3.4 De werking van STARTTLS. 14
3.5 De door STARTTLS versleutelde links bij het verzenden van een e-mail (rood). 15
3.6 DANE vanuit een top-levelbenadering. 17
3.7 Een voorbeeld van phishing. 19

4.1 De verhouding tussen de artt. 25 en 32 Avg. 29

Lijst van tabellen

3.1 Bereikte securitydoelen door het protocol van de Coalitie. . . . 21

Inhoudsopgave

1 Inleiding **5**

2 Voorkennisvereisten **8**

3 Vervulde securitydoelen door het protocol **9**

3.1 Voorkennis 10
3.1.1 Het Simple Mail Transfer Protocol (SMTP) 10
3.1.2 Asymmetrische cryptografie 11
3.1.3 Domain Name System (DNS) 12
3.2 STARTTLS 13
3.2.1 Werking 14
3.2.2 Securitydoelen van STARTTLS 15
3.3 Domain Name System Security Extensions (DNSSEC) 16
3.3.1 Werking 16
3.3.2 Securitydoelen van DNSSEC 16
3.4 DNS-based Authentication of Named Entities (DANE) 17
3.4.1 Werking 17
3.4.2 Securitydoelen van DANE 18
3.5 Sender Policy Framework (SPF) 19
3.5.1 Werking 19
3.5.2 Securitydoelen van SPF 20
3.6 Domain Keys Identified Mail (DKIM) 20
3.6.1 Werking 20
3.6.2 Securitydoelen van DKIM 20
3.7 Domain-based Message Authentication, Reporting and Conformance (DMARC) 21
3.7.1 Werking 21
3.7.2 Securitydoelen van DMARC 21
3.8 Conclusie 21

4 Plichten uit de Verordening **22**
4.1 Toepassingsbereik 22
4.1.1 Grensoverschrijdend effect 23
4.1.2 Materiële omvang: art. 2 juncto 4 Avg 23
4.1.3 Territoriale omvang: art. 3 juncto 4 Avg 24
4.2 De relevante plichten uit de Avg 24
4.3 De omvang van de plichten uit de Avg 26
4.3.1 De samenloop tussen de plichten uit de Avg 28
4.4 Toepassing 29
4.4.1 Risico 29
4.4.2 De aard, omvang, context en de doeleinden van de verwerking 30
4.4.3 De stand van de techniek 30
4.4.4 De uitvoeringskosten 30
4.5 Conclusie 31
4.5.1 Afweging 31
4.5.2 Conclusie 31

5 Verwant werk **32**

6 Conclusies **33**
6.1 Securitydoelen: samenvatting 33
6.2 Plichten uit de Avg: samenvatting 35
6.3 Conclusie 36
6.4 Discussie 36
6.5 Suggestie ter verbetering 39

Bibliografie **41**

Hoofdstuk 1

Inleiding

Een tijd geleden kwam ik uit op een voor mij interessante website (hierna: "de website") van Forum Standaardisatie.[1] De website beschrijft twee gevaren. Ten eerste kunnen e-mails worden afgetapt door (mogelijk kwaadwillende) derden. Deze derden kunnen vervolgens de inhoud van de e-mailberichten lezen, omdat e-mails volgens de website onversleuteld worden verzonden. Met andere woorden, kwaadwillenden kunnen de door hen afgetapte e-mails afluisteren. Er blijkt echter nog een tweede gevaar uit de beschrijving op de website. Ontvangers krijgen namelijk e-mails terwijl zij niet zeker weten of het e-mailadres van de ontvangen e-mail daadwerkelijk aan de verzender daarvan toebehoort. Verzenders kunnen mogelijk hun identiteit manipuleren en met die identiteit e-mails verzenden onder een andere naam, met als doel het afhandig maken van geheime financiële gegevens. Dat wordt phishing genoemd. De website geeft zelf geen definitie van het woord phishing, maar gebruikt dat woord wel. De website beschrijft een protocol (hierna: "het protocol") dat moet beschermen tegen afluisteren en phishing, als een manier om de eerder beschreven gevaren te bestrijden. Het probleem waar ik op stuit is echter dat het mij niet duidelijk is hoe *effectief* het protocol die gevaren bestrijdt.

Vanaf mei 2018 is een nieuw stuk privacywetgeving van kracht, de Algemene verordening gegevensbescherming (hierna: "de Verordening" of "de Avg").[2] De Verordening poogt het gegevensbeschermingsrecht te harmonise-

[1] Forum Standaardisatie is een Nederlands overheidsorgaan. Zie voor de website Forum Standaardisatie, "Nederland zorgt voor veilig e-mailverkeer", 02-feb-2017. [Online]. Beschikbaar op: https://www.forumstandaardisatie.nl/nieuws/nederland-zorgt-voor-veilig-e-mailverkeer. [Geraadpleegd: 28-mrt-2017].

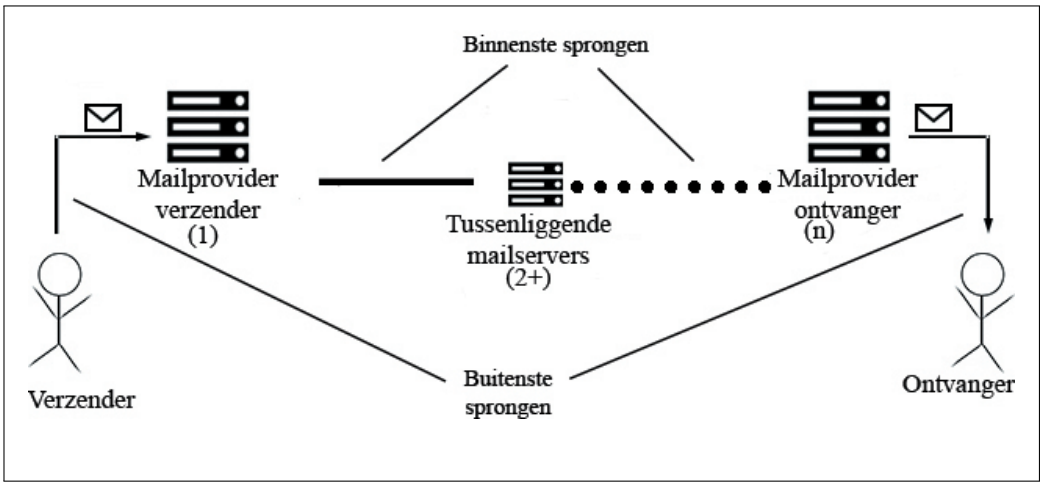
[2] Verordening 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming).

ren. Op basis van deze informatie over de Verordening en het probleem dat ik in de vorige alinea uitwerkte komt bij mij de onderzoeksvraag van deze scriptie op. Ik vraag mij namelijk af of het protocol effectief genoeg is voor de Coalitie om te voldoen aan de plichten, die voortvloeien uit de bepalingen van de Verordening. De onderzoeksvraag van deze scriptie luidt daarom: *welke voor de Coalitie relevante plichten vloeien voort uit de bepalingen van de Algemene verordening gegevensbescherming, en in hoeverre voldoen de partijen in de Coalitie aan die plichten door het protocol te implementeren?*

Er bestaat weinig duidelijkheid over de gevolgen van de invoering van de Verordening. Uit de Verordening komen immers mogelijk nieuwe rechten en plichten op voor allerlei partijen. Door het uitwerken van de centrale vraag beoog ik enkele van de gevolgen van de invoering van de Verordening duidelijker zichtbaar te maken. Deze scriptie bevat dan ook een praktische toepassing van enkele nieuwe plichten uit de Verordening op de Coalitie en het protocol. Gezien het voorgaande is deze scriptie relevant voor de rechtspraktijk, waaronder de bedrijven die vallen onder de reikwijdte van de Verordening.

Hoofdstukken 3 en 4 beantwoorden de eerder uitgewerkte onderzoeksvraag. Hoofdstuk 6 geeft de conclusies die kunnen worden afgeleid uit die hoofdstukken weer. De eindconclusie luidt dat de partijen in de Coalitie niet voldoen aan de eisen die de Verordening stelt, ook al is meer jurisprudentie vereist om die eindconclusie buiten redelijke twijfel te kunnen bevestigen. Uiteindelijk geef ik een aantal maatregelen weer die die situatie behoren te verbeteren, gevolgd door mijn uit die maatregelen gekozen persoonlijke voorkeur.

Op de volgende pagina staat een lijst met definities die in de rest van deze scriptie gebruikt zullen worden. Het plaatje erboven geeft de terminologie weer tijdens het mailproces. Het getal n in de figuur is groter dan of gelijk aan 2.



Versleuteling over meerdere sprongen	Versleuteling op elk deel van de link tussen de verzender en de ontvanger
De binnenste sprongen	De sprongen tussen de e-mail service providers
De buitenste sprongen	De sprongen tussen de service provider en de eindgebruiker aan zowel de verzendende als de ontvangende zijde
Ontwikkel- en productiefase	De fase tussen het begin van de ontwikkeling van een nieuw product en de verwerking van persoonsgegevens
Verwerkingsfase	De fase waarin het verwerken van persoonsgegevens begint
Privacy by design-plicht	De gecodificeerde plicht in art. 25 Avg
Plicht tot bescherming van persoonsgegevens	De gecodificeerde plicht in art. 32 Avg

Hoofdstuk 2

Voorkennisvereisten

Deze scriptie is geschreven met het niveau van een gemiddelde eerstejaars informaticastudent in gedachte. De scriptie bevat ook specialistische juridische kennis in hoofdstuk 4. Om dat hoofdstuk volledig te kunnen begrijpen is een introductievak in het recht mogelijk vereist. Deze scriptie vereist, met andere woorden, ook een basaal begrip van de werking van het recht.

Hoofdstuk 3

Vervulde securitydoelen door het protocol

Het protocol beoogt, zoals ik in de inleiding ook al zei, te beschermen tegen phishing en afluisteren. Om meer te weten te komen over de werking en veiligheid van het protocol, zodat ik het kan toetsen aan de Avg, zal ik daarom in dit hoofdstuk onderzoeken welke van de securitydoelen Confidentiality, Integrity en Authentication het protocol behaalt. Confidentiality staat voor de mogelijkheid om berichten vertrouwelijk te houden. Integrity staat voor de mogelijkheid om de inhoud van een bericht te wijzigen. Authentication gaat over het vermogen om de identiteit van partijen te kunnen achterhalen.[4, p. 3–8]

In de securitywereld is het gebruikelijk om onderzoek te doen naar de doelen Confidentiality, Integrity en *Availability*.[4, p. 3–8] Normaal gesproken zou ook het doel Availability dus relevant zijn, maar gelet op het doel van het protocol - het voorkomen van phishing en afluisteren - lijkt Availability mij minder relevant. Het securitydoel Availability gaat er namelijk over in hoeverre de werking van een dienst kan worden verstoord door kwaadwillende derden. Dat heeft minder te maken met phishing en afluisteren dan de andere hier besproken securitydoelen, en meer te maken met het mogelijk maken van een werkend e-mailsysteem. Daarom beperk ik mij in deze scriptie tot de doelen Confidentiality, Integrity en Authentication (In deze scriptie: "C.I.A."). Confidentiality heeft namelijk rechtstreekt te maken met het al dan niet kunnen afluisteren van berichten. Integrity heeft ermee te maken dat afgeluisterde berichten kunnen worden veranderd, en is daarom relevant. Authentication heeft met phishing van doen, phishing heeft namelijk te maken met de mate waarin de identiteit van een partij kan worden achterhaald. Voor phishing is immers vereist dat de identiteit van de verzender kan worden vervalst en misbruikt voor het achterhalen van geheime

financiële gegevens.

In paragraaf 3.1 zal ik allereerst de vereiste voorkennis geven voor een beter begrip van het protocol. Het protocol bestaat uit de standaarden STARTTLS, DNSSEC, DANE, SPF, DKIM en DMARC. In de paragrafen die volgen op paragraaf 3.1 zal ik per standaard van het protocol uitleggen hoe de standaard werkt en welke securitydoelen de standaard behaalt. In paragraaf 3.8 vat ik de conclusies van dit hoofdstuk tot slot samen in een tabel.

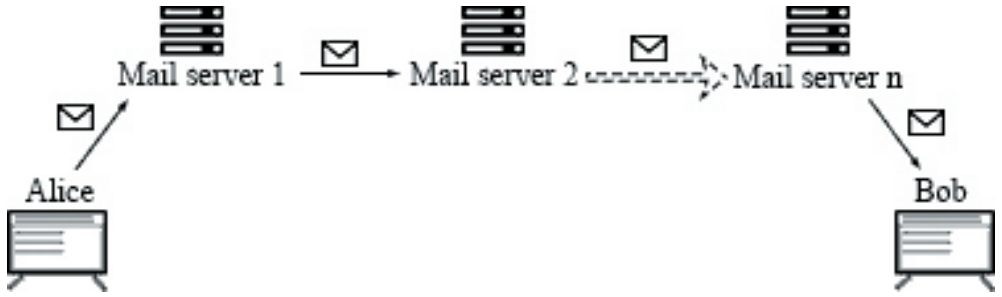
3.1 Voorkennis

In deze paragraaf bespreek ik de vereiste voorkennis van dit hoofdstuk. paragraaf 3.1.1 geeft de werking van e-mail door middel van een beschrijving van het protocol SMTP. Ik bespreek asymmetrische cryptografie als voorkennis van STARTTLS in de subparagraaf daarna. Tot slot wordt de werking van DNS als voorkennis van DNSSEC in paragraaf 3.1.3 beschreven.

3.1.1 Het Simple Mail Transfer Protocol (SMTP)

SMTP is gemaakt om gebruikt te worden door mailclients en regelt de globale manier waarop e-mails worden verstuurd en ontvangen. Een voorbeeld van zo'n mailclient is Microsoft Outlook. SMTP kent twee clients, de verzender en de ontvanger. De verzender zal proberen een e-mail te versturen naar de ontvanger, van wie hij vóór de verzending al het e-mailadres wist. SMTP zal proberen de e-mail te bezorgen bij het IP-adres van de ontvanger, langs twee of meer mailservers.[9] Hij gebruikt het e-mailadres van de ontvanger om dat IP-adres te achterhalen. E-mailadressen worden vertaald naar IP-adressen via DNS, omdat een computer een e-mailalias niet begrijpt maar e-mailadressen wel.[3]. De e-mail wordt via twee of meer mailservers sprongsgewijs bezorgd bij de ontvanger.[9] Er is in de praktijk vaak geen mailserver tussen de mailservers van de mailproviders van de verzender en de ontvanger.[12, p. 122] Echter, de RFC die de SMTP definieert sluit meer dan twee sprongen niet uit.[9, par. 2.1] De hier beschreven situatie wordt getoond in de figuur op de volgende pagina.

[3] Zie paragraaf 3.1.3 voor meer informatie over die vertaling.



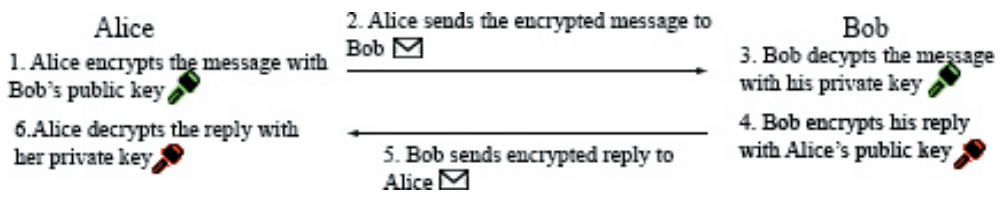
Figuur 3.1: Een mogelijk SMTP-sessie tussen Alice (verzender) en Bob (ontvanger).

In de figuur hierboven probeert Alice een e-mail te sturen naar Bob, via twee of meer tussenliggende mail servers. Die servers worden in de figuur aangegeven met getallen 1 tot en met n, met n een getal groter of gelijk aan 2.

De e-mail wordt, gelet op het voorgaande, op sprongsgewijze basis naar de ontvanger van het bericht verstuurd. In paragraaf 3.2.2 kom ik erachter dat die basis effect heeft op de beveiliging van e-mail. Meer over het effect van het sprongsgewijs versturen van e-mails op de beveiliging van die e-mails is gegeven in die paragraaf.

3.1.2 Asymmetrische cryptografie

Bij asymmetrische cryptografie wordt een bericht versleuteld met twee sleutels. De ene in de publieke sleutel, de andere is de geheime sleutel. De publieke sleutel is bestemd om openbaar te worden gemaakt zodat een verzender een bericht ermee kan versturen. De geheime sleutel is bestemd voor het ontsleutelen van het bericht en moet dus absoluut geheim blijven. Bij asymmetrische cryptografie zijn de publieke en de geheime sleutel wiskundig van aard. De figuur op de volgende pagina geeft een voorbeeld van hoe asymmetrische cryptografie in de praktijk werkt.



Figuur 3.2: Een voorbeeld van het uitwisselen van berichten middels asymmetrische versleuteling.

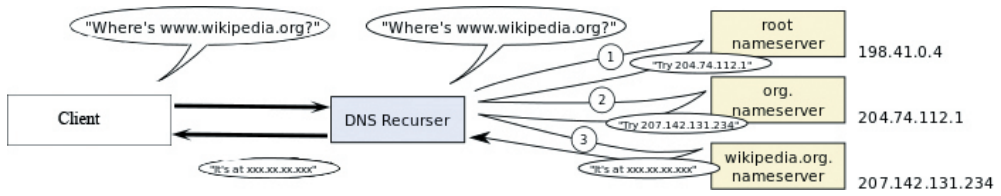
In de figuur hierboven wil Alice versleuteld berichten uitwisselen met Bob. Alice versleutelt het bericht met behulp van Bobs publieke sleutel (in de figuur: stap 1). Zij stuurt het versleutelde bericht aan Bob (in de figuur: stap 2). Bob ontsleutelt het bericht met behulp van zijn geheime sleutel (in de figuur: stap 3). Bob doet de vorige drie stappen analoog voor zijn antwoord aan Alice (stappen 4, 5 en 6).

STARTTLS maakt gebruik van asymmetrische cryptografie om de versleuteling tussen partijen te starten. Meer over die toepassing in paragraaf 3.2.1.

3.1.3 Domain Name System (DNS)

Zoals beschreven in paragraaf 3.1.1 gebruikt SMTP het Domain Name System (afgekort DNS) om te achterhalen welk IP-adres bij het e-mailadres van de ontvanger hoort. Daarom beschrijf ik de werking van DNS in deze paragraaf.

DNS kan worden gezien als een database voor het opslaan en ophalen van de informatie die tot een domain behoort. Het IP-adres dat bij een bepaalde domeinnaam hoort wordt opgezocht door van het achterste deel van de domeinnaam naar het voorste deel telkens servers te benaderen en te vragen naar hun IP-adres. De volgende figuur geeft die werking door middel van een voorbeeld weer.



Figuur 3.3: Een voorbeeld van het opzoeken van een IP-adres dat bij een bepaalde domeinnaam hoort.

In de figuur hierboven wordt het IP-adres dat hoort bij www.wikipedia.org opgezocht door een client (in het geval van e-mail dus de mailclient, zie paragraaf 3.1.1). Eerst wordt de "root server", een bekende server, benaderd door de DNS Recurser (een programma dat DNS-queries oplost). De root server stuurt het IP-adres van de .org-server als antwoord terug naar de recurser. De .org-server doet hetzelfde voor de wikipedia.org server. Uiteindelijk stuurt de wikipedia.org-server zijn IP-adres terug naar de recurser, die het IP-adres terugstuurt naar de client. Nu heeft de client het IP-adres van wikipedia.org en kan de e-mail naar die server worden verstuurd met dat IP-adres.

Een geschikte analogie van DNS lijkt mij een ouderwets telefoonboek. In een telefoonboek zou men iemands telefoonnummer opzoeken, want met een naam-adres-woonplaatscombinatie kan een telefoon niet bellen. Stapsgewijs wordt met behulp van het telefoonboek het telefoonnummer opgezocht, net als bij DNS.

In paragraaf 3.3.2 kom ik erachter dat het feit dat e-mail DNS gebruikt voor het opzoeken van de bestemming van de e-mail ervoor zorgt dat DNSSEC - dat DNS beveiligt - een securitydoel behaalt. Zie voor meer daarover de desbetreffende paragraaf.

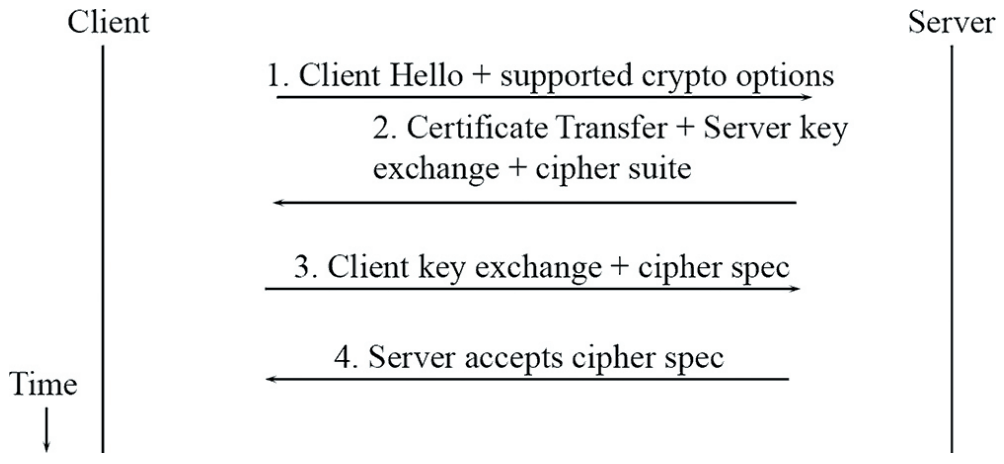
3.2 STARTTLS

Het protocol bestaat, zoals eerder gezegd, uit STARTTLS, DNSSEC, DANE, SPF, DMARC en DKIM. Vanaf deze paragraaf zal ik per standaard waaruit het protocol bestaat uitwerken hoe het protocol werkt, gevolgd door de securitydoelen die het protocol gelet op die werking bereikt voor e-mail.

3.2.1 Werking

Voor SMTP is het gebruik van STARTTLS volledig optioneel.[7] Partijen kiezen dus zelf of zij ervan gebruik maken. STARTTLS kan worden gebruikt om van een onveilige verbinding een beveiligde verbinding te maken. Het doet dat op twee manieren: het versleutelen van berichten, en het opzetten van een veilige TLS-"tunnel" waardoor berichten worden verzonden en niet meer kunnen worden aangepast onderweg. Ik ga er in het verloop van deze scriptie van uit dat die tunnel veilig is. Bovendien blijkt uit onderzoek van bijvoorbeeld Krawczyk e.a. dat een TLS-verbinding relatief veilig is.[10] Ik zal dus niet verder ingaan op de veiligheid van de TLS-"tunnel". Ik zal wel ingaan op hoe STARTTLS werkt.

STARTTLS gebruikt asymmetrische versleuteling om de eerder besproken veilige tunnel tot stand te brengen.



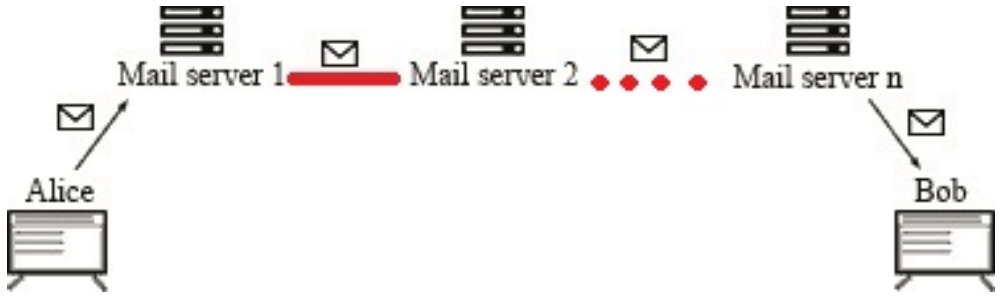
Figuur 3.4: De werking van STARTTLS.

In de figuur hierboven wisselen client en server de nodige informatie uit om een TLS-"tunnel" op te zetten. Er worden publieke en geheime sleutels uitgewisseld voor de in paragraaf 3.1.2 uitgewerkte versleuteling. Ook worden certificaten uitgewisseld zodat client en server tijdens het opzetten van de tunnel met elkaar berichten uitwisselen en niet met een derde.[10, p. 3] Ik ga er verder niet op in hoe die certificaten gebruikt en geverifieerd worden, maar ga ervan uit dat die verificatie goed gebeurt, omdat de wijze van controle mij niet relevant lijkt voor de securitydoelen van e-mail.

Het probleem met de in de vorige alinea beschreven uitwisseling is dat

een kwaadwillende derde een antwoord naar de client kan sturen - vóór stap 2 - waarin staat dat er geen versleuteling gebruikt zal worden. De client verstuurd dan onversleuteld de informatie naar de server, en de kwaadwillende derde kan de berichten die worden uitgewisseld tussen client en server dan afluisteren. Er wordt dan helemaal geen beveiligde verbinding gebruikt. Een RFC beschrijft dit probleem.[8, par. 2.2] In paragraaf 3.4.1 leg ik uit hoe DANE dat probleem oplost.

3.2.2 Securitydoelen van STARTTLS



Figuur 3.5: De door STARTTLS versleutelde links bij het verzenden van een e-mail (rood).

Uit de figuur hierboven blijkt tussen welke partijen het protocol versleuteling afdwingt. De rode (stippel)lijnen in de figuur geven aan op welke links tussen verzender en ontvanger versleuteling en een beveiligde TLS-"tunnel" wordt opgezet door het protocol. De versleuteling zorgt voor Confidentiality omdat de e-mail niet meer kan worden ingezien op de versleutelde links. De TLS-"tunnel" zorgt voor Integrity, omdat e-mails die binnen de tunnel verstuurd worden niet door kwaadwillende derden kunnen worden aangepast in die tunnel. In paragraaf 3.4.2 kom ik er achter dat het protocol STARTTLS slechts op de binnenste sprongen gebruikt. De buitenste sprongen zijn door het protocol niet beveiligd. Ik concludeer daarom dat STARTTLS in het geval van het protocol zorgt voor *binnenste sprong Confidentiality* en *binnenste sprong Integrity*.

3.3 Domain Name System Security Extensions (DNSSEC)

3.3.1 Werking

DNSSEC beveiligt DNS door middel van een zogenoemde "vertrouwensketen", beginnend bij de root server.[4] Net als in figuur 3.1.3 gaat DNSSEC van boven naar beneden te werk. Bij DNSSEC krijgt de recurser echter een certificaat terug waarmee hij kan controleren of de volgende server die hij vraagt echt is wie hij zegt te zijn. Zo kan de recurser controleren of een kwaadwillende derde probeert het antwoord op zijn queries te veranderen.

Het certificaat van de rootserver heeft de recurser al. De rootserver geeft het certificaat van de volgende server (in figuur 3.1.3 de .org server), enzovoort totdat het antwoord op de hele query (in figuur 3.1.3 het IP-adres van wikipedia.org) is gegeven.[2, p. 48] Ik ga ervan uit dat de controle en het ondertekenen van de certificaten goed verloopt. De kern van de hier gegeven beschrijving is dat DNSSEC ervoor zorgt dat DNS veilig gebruikt kan worden: een kwaadwillende derde kan zich niet voordoen als DNS-server, omdat zijn server niet in de vertrouwensketen zit.[6]

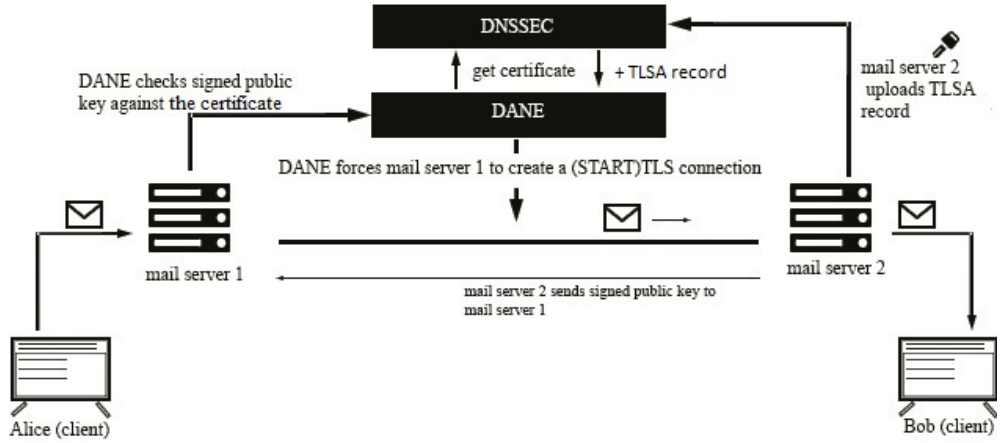
3.3.2 Securitydoelen van DNSSEC

DNSSEC zorgt ervoor, gelet op de werking beschreven in de vorige paragraaf en het beschrevene in paragraaf 3.1.1, dat het IP-adres van de ontvanger met behulp van het e-mailadres veilig kan worden opgezocht zonder dat het kan worden veranderd. DNSSEC behaalt dus *Integrity van de bestemming*.

[4] Zie bijvoorbeeld figuur 3.1.3 voor informatie over welke server bedoeld wordt.

3.4 DNS-based Authentication of Named Entities (DANE)

3.4.1 Werking



Figuur 3.6: DANE vanuit een top-levelbenadering.

In paragraaf 3.2.1 werd uitgelegd dat STARTTLS-versleuteling kan worden omzeild doordat een kwaadwillende derde een bericht kan sturen aan de cliënt waarin staat dat geen versleuteling wordt gebruikt. DANE poogt deze versleuteling alsnog af te dwingen tussen de mailservers, met behulp van DNSSEC-beveiligde DNS. DANE dwingt de mailservers in figuur 3.1.1 dus om onderling versleuteling te gebruiken voor verstuurde e-mails. De ontvangende mail server zet in een speciaal "TLSA record", in DNS, dat TLS wordt ondersteund. Ook staat het certificaat van de publieke sleutel in DNS, zodat de verzendende mailserver kan controleren of de publieke sleutel klopt.[3, p. 2900] Wie dat certificaat in DNS kan zetten en hoe de certificaatcontrole plaatsvindt lijkt mij verder irrelevant voor deze scriptie.

DANE kijkt vanuit de kant van de verzender of de ontvanger TLS ondersteunt, door dat op te zoeken in DNS. Ook controleert DANE de publieke sleutel die de ontvangende mail server heeft gestuurd voor de asymmetrische versleuteling van de e-mail. Als er geen TLSA record kan worden gevonden in DNS, dan probeert DANE een traditionele STARTTLS verbinding aan te gaan met de betreffende server, op de manier zoals uitgelegd in paragraaf

3.2.1. Als de ontvangende server aangeeft dat er geen versleuteling is terwijl dat volgens het door DANE opgehaalde TLSA record wel zo is, dan wordt er geen verbinding gemaakt.[3, p. 2900] Deze situatie wordt in de figuur aan het begin van deze paragraaf weergegeven.

3.4.2 Securitydoelen van DANE

DANE gebruikt, zoals in de vorige paragraaf uiteengezet, DNSSEC om ervoor te zorgen dat STARTTLS tussen servers wordt afgedwongen. Op de links tussen servers kan dus niet worden afgeluisterd, want er is een beveiligde TLS-"tunnel" op die links. DANE behaalt daardoor *binnenste sprong Confidentiality* en *binnenste sprong Integrity*. Ook controleert DANE de identiteit van de ontvangende mail server met behulp van het TLSA record en het certificaat van de publieke sleutel uit DNS. De identiteit van de ontvangende mail server wordt dus achterhaald. DANE behaalt dus ook *binnenste sprong ontvangende mail server Authentication*.

3.5 Sender Policy Framework (SPF)

3.5.1 Werking

From: vaish02@stanford.edu
<vaish02@stanford.edu>
Subject: (@MS ; Recruitment~2016/2025)

MEMBER
MSPA®
MYSTERY SHOPPING
PROVIDERS ASSOCIATION

Department for Employment & Learning,
We are seeking to identify a pool of skilled evaluators.

REPRESENTATIVE DUTIES:
Reviews and surveys for collection-of-data.
You just conducting project evaluation.
You need to be collecting and analyzing primary data.

REQUIREMENTS:
 # 18 year old or above.
 # Can read and write english.
 # No experience needed like shopping.

PAYMENTS:
 # You will get $355(USD) each assignment.
 # Most of the time you will only need to spend 20-30 minutes on the visit.

Figuur 3.7: Een voorbeeld van phishing.

Zoals blijkt uit paragraaf 3.1.1 heeft SMTP geen Authentication van de verzender. De identiteit van de verzender wordt niet achterhaald, en daarom kunnen phishingmails zoals in figuur 3.7 worden verstuurd. Bij de e-mail in die figuur probeert de verzender zich voor te doen als iemand van Stanford University, om namens de Mystery Shopping Providers Association een baan aan te bieden aan de ontvanger. Het doel achter deze e-mail is het achterhalen van geheime financiële gegevens van de ontvanger.

SPF probeert authentication van de verzender - in tegenstelling tot SMTP - wél toe te voegen. Op die manier wordt mail spoofing (het manipuleren van het verzendende e-mailadres) bemoeilijkt. Het is immers moeilijk voor een aanvaller om een e-mailadres te manipuleren als kan worden aangetoond dat die aanvaller niet bevoegd is om de e-mail te versturen. SPF werkt vanaf de zijde van de ontvanger van de e-mail. SPF gebruikt DNS om het IP adres van het domein achter het e-mailadres van de ontvangen e-mail te achterhalen, en

zo te controleren of de verzender bevoegd is om e-mails namens dat domein te versturen. Een voorbeeld. Stel dat een e-mailadres ontvangen wordt van het IP-adres van billing@paypal.com. In een SPF record staat in DNS echter dat e-mails slechts worden verstuurd van het IP-adres van service@paypal.com. In dat geval wordt de e-mail geweigerd. In andere gevallen wordt de e-mail toegelaten. Als er geen SPF record bestaat voor het betreffende domein, dan wordt de e-mail toegelaten.[19]

3.5.2 Securitydoelen van SPF

SPF controleert slechts of het IP-adres van de ontvangen e-mail bevoegd is om e-mails namens het domein van die e-mail te versturen. SPF zorgt dus voor *domain Authentication van de verzender.*

3.6 Domain Keys Identified Mail (DKIM)

3.6.1 Werking

DKIM gebruikt, net als SPF, DNS-informatie om ontvangen e-mails te controleren. Echter controleert DKIM of de e-mail zelf is gewijzigd. De e-mailprovider van de verzender voegt een DKIM-certificaat toe aan de e-mail, dat hij heeft geüpload naar DNS. Vervolgens controleert DKIM aan de zijde van de ontvanger of het certificaat in de ontvangen e-mail en het certificaat in DNS overeenkomen. Hoe die controle of het uploaden naar DNS plaatsvindt lijkt mij verder irrelevant voor deze scriptie. Van belang is dat DKIM kijkt of het certificaat nog klopt. Het idee is dat alleen de e-mailprovider van de verzender het certificaat kan toevoegen.[15, p. 3]

3.6.2 Securitydoelen van DKIM

DKIM controleert een certificaat. De buitenste sprongen zijn echter niet versleuteld, en elke mail server tussen de serviceproviders kunnen de e-mail inzien en wijzigen, zoals blijkt uit paragrafen 3.4.2 en 3.2.2. Elke mailserver tussen de verzender en de ontvanger kan de e-mail wijzigen en het certificaat hergebruiken. Ook kwaadwillende derden op de buitenste sprongen kunnen dat doen, omdat die sprongen niet versleuteld zijn. Daarom behaalt DKIM *Integrity tussen de verzendende mail provider en de ontvanger in de binnenste sprongen.*

3.7 Domain-based Message Authentication, Reporting and Conformance (DMARC)

3.7.1 Werking

DMARC combineert SPF en DKIM en geeft een aantal opties om SPF en DKIM makkelijker te gebruiken. DMARC geeft bovendien rapporten met statistieken over bijvoorbeeld het aantal geblokkeerde phishingmails en spammails.[15, p. 3]

3.7.2 Securitydoelen van DMARC

DMARC stuurt rapporten, maar voegt verder niets toe aan de beveiliging die SPF en DKIM samen bieden. Dat komt omdat DMARC gebruik maakt van SPF en DKIM voor de beveiliging. Daarom behaalt DMARC slechts de securitydoelen beschreven in paragrafen 3.5.2 en 3.6.2.

3.8 Conclusie

De onderstaande tabel geeft per standaard van het protocol weer welke van de doelen Confidentiality, Integrity en Authentication door die standaard bereikt zijn. Voor de ratio achter deze tabel verwijs ik naar de voorgaande paragrafen, die de doelen per standaard bespreken.

Tabel 3.1: Bereikte securitydoelen door het protocol van de Coalitie.

				DMARC	
	STARTTLS	**DNSSEC**	**DANE**	**SPF**	**DKIM**
Bereikte securitydoelen	• Binnenste sprong Confidentiality • Binnenste sprong Integrity	Integrity van de bestemming	• Binnenste sprong Confidentiality • Binnenste sprong Integrity • Binnenste sprong ontvangende mail server Authentication	Domain Authentication van de verzender	Integrity tussen versturende mail provider en ontvanger in de binnenste sprongen

Hoofdstuk 4

Plichten uit de Verordening

In de inleiding stelde ik de onderzoeksvraag van deze scriptie. Die vraag luidt: *welke voor de Coalitie relevante plichten vloeien voort uit de bepalingen van de Algemene verordening gegevensbescherming, en in hoeverre voldoen de partijen in de Coalitie aan die plichten door het protocol te implementeren?* In dit hoofdstuk zal ik een antwoord geven op die onderzoeksvraag.

Wat het protocol is en hoe veilig het is blijkt uit het vorige hoofdstuk. In dit hoofdstuk zal ik eerst beoordelen of de Avg van toepassing is in het geval van het protocol. Dat gebeurt in paragraaf 4.1. Daarna leid ik de relevante plichten uit de Avg af in paragraaf 4.2. Paragraaf 4.3 gaat in op de inhoud van de plichten, dat wil zeggen, wat de omvang van de plichten is. Tot slot worden in paragraaf 4.4 de in paragraaf 4.2 gevonden plichten uit de Avg toegepast. In de in deze alinea genoemde paragrafen zullen de volgende artikelen achtereenvolgens worden toegepast:

- Art. 2 juncto 4 Avg
- Art. 3 juncto Avg
- Art. 95 Avg
- Art. 32 Avg
- Art. 25 Avg

4.1 Toepassingsbereik

Eerst dus het toepassingsbereik. Het Europese recht is slechts van toepassing in het geval een grensoverschrijdend effect aanwezig is. Dat betekent dat er een effect moet zijn op de tussenstaatse Europese handel, anders is het

Europese recht niet van toepassing.[14, p. 147] In paragraaf 4.1.1 controleer ik of er een grensoverschrijdend effect is. Paragraaf 4.1.2 controleert of de Avg van toepassing is aan de hand van de materiële omvang van de Avg, gegeven in art. 2 Avg. Paragraaf 4.1.3 controleert of de coalitie binnen de territoriale reikwijdte van de Avg valt, gegeven in art. 3 Avg.

4.1.1 Grensoverschrijdend effect

Het besproken geval in deze scriptie gaat over e-mail. E-mails kunnen de grens over gaan en de daarmee samenhangende persoonsgegevens, zoals bijvoorbeeld IP-adressen of gevoeligere informatie, ook.[5] Als zulke persoonsgegevens door een confidentialityfout openbaar worden gemaakt, dan kan dat bijvoorbeeld de tussenstaatse handel belemmeren vanwege reputatieschade. Er is dus sprake van een grensoverschrijdend effect. Het Europese recht is daarom van toepassing op dit geval.

4.1.2 Materiële omvang: art. 2 juncto 4 Avg

Is de Avg van toepassing op specifiek het in deze scriptie beschreven protocol? Daarvoor wordt in deze paragraaf gekeken naar art. 2 Avg. Dat artikel luidt:

> " Deze verordening is van toepassing op de geheel of gedeeltelijk *geautomatiseerde verwerking*, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen."

Art. 4 Avg geeft definities over de onderstreepte elementen. Volgens art. 4 sub 2 Avg is de *verwerking* een bewerking, al dan niet via geautomatiseerde procedés. Dat artikel geeft een groot aantal voorbeelden van zo'n bewerking. Daaronder valt het verzamelen en verstrekken door middel van doorzending van *persoonsgegevens*. Onder *persoonsgegevens* valt volgens art. 4 sub 1 Avg alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

In casu betreft het een geautomatiseerde verwerking, omdat er een bewerking wordt uitgevoerd op persoonsgegevens. Er wordt bijvoorbeeld IP-informatie doorgestuurd bij elke e-mail, zo blijkt uit paragraaf 3.1.1. Via een IP-adres is een natuurlijk persoon identificeerbaar. Elk versturen van een e-mail betreft daarom een verwerking van persoonsgegevens. Het protocol doet deze verwerking bovendien volledig *automatisch*. In casu betreffen de

[5] Ook een IP-adres is een persoonsgegeven. Met een IP-adres kan immers de identiteit van een persoon worden achterhaald.[11, p. 36 en 38]

bewerkingen die het protocol maakt dus een *geautomatiseerde verwerking*. De werking van het protocol valt daarom binnen de materiele omvang beschreven in art. 2 Avg.

4.1.3 Territoriale omvang: art. 3 juncto 4 Avg

Art. 3 Avg geeft de territoriale reikwijdte van de Avg, en geeft in feite aan of de Avg van toepassing is op de partijen van de Coalitie. Volgens art. 3 gaat het daarbij om een verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een *verwerkingsverantwoordelijke* of een *verwerker* in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt. Voor de territoriale omvang is een verwerkingsverantwoordelijke of verwerker in de Unie dus vereist. Volgens art. 4 sub 7 Avg is een verwerkingsverantwoordelijke een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, *alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*. De partijen in de coalitie stellen allemaal het doel en de middelen van de verwerking vast, zo blijkt uit hun plan. Zij zijn bovendien rechtspersonen. Zij zijn daarom verwerkingsverantwoordelijken. Art. 4 sub 8 definieert een verwerker als een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voor zover de partijen in de coalitie zelf de persoonsgegevens verwerken zijn zij daarom ook verwerkers. Ook zijn zij allen rechtspersonen gevestigd in Nederland. Aan de territoriale omvang van de Avg is voldaan, omdat de partijen in de coalitie in de unie gevestigde verwerkingsverantwoordelijken zijn. Ook zijn zij soms in de unie gevestigde verwerkers, afhankelijk van of zij hun eigen mailservers zelf beheren of niet. De Avg is dus van toepassing op de partijen van de Coalitie.

4.2 De relevante plichten uit de Avg

Op basis van de Avg-bepalingen kan ik in ieder geval twee van toepassing zijnde plichten vinden. Dat zijn de beveiligingsplichten gecodificeerd in art. 32 en art. 25 Avg. Art. 32 Avg gaat namelijk over de plicht tot beveiliging van persoonsgegevens, art. 25 Avg omhelst een algemenere plicht tot het nemen van maatregelen zowel voor als tijdens de verwerking van persoonsgegevens.[6] Beide artikelen zijn van toepassing op verwerkingsver-

[6] Meer over de omvang van de plichten uit artt. 25 en 32 is te vinden in paragraaf 4.3.

antwoordelijken en leggen hen verplichtingen op, daarom zijn beide artikelen van toepassing op de partijen van de Coalitie.[7]

Er is nog een derde mogelijke plicht die zou kunnen worden afgeleid uit de Avg. Die plicht blijkt uit het bepaalde in art. 95 Avg. Dat artikel luidt als volgt:

> "Deze verordening legt natuurlijke personen of rechtspersonen geen aanvullende verplichtingen op met betrekking tot verwerking in verband met het verstrekken van openbare elektronische-communicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van *Richtlijn 2002/58/EG* onderworpen zijn aan *specifieke verplichtingen met dezelfde doelstelling.*"

De verordening is dus niet van toepassing op partijen van de Coalitie voor zover op grond van Richtlijn 2002/58/EG dezelfde specifieke verplichting voor die partijen geldt met dezelfde inhoud en doelstelling. Zo'n verplichting blijkt uit art. 4 van richtlijn 2002/58/EG. Art. 32 Avg bouwt natuurlijk voort op art. 4 van die richtlijn: beide artikelen hebben tot doel persoonsgegevens te beschermen en hebben soortgelijke criteria.

De wetgever verheldert art. 95 Avg enigszins in overweging 173:

> "Deze verordening dient van toepassing te zijn op alle aangelegenheden die betrekking hebben op de bescherming van grondrechten en fundamentele vrijheden in het kader van de verwerking van persoonsgegevens waarvoor de in Richtlijn 2002/58/EG van het Europees Parlement en de Raad (2) opgenomen specifieke verplichtingen met dezelfde doelstelling niet gelden, met inbegrip van de verplichtingen van de verwerkingsverantwoordelijke en de rechten van natuurlijke personen. Om de verhouding tussen deze verordening en Richtlijn 2002/58/EG te verduidelijken, dient die richtlijn dienovereenkomstig te worden gewijzigd. *Zodra deze verordening is vastgesteld, dient Richtlijn 2002/58/EG te worden geëvalueerd, met name om te zorgen voor samenhang met deze verordening*"

Aangezien de wetgever art. 95 Avg heeft gemaakt als een tijdelijke maatregel om de verhouding tussen beide Richtlijn 2002/58/EG en de Avg te bepalen, zoals uit het in dit citaat schuingedrukte deel blijkt, zal ik die richtlijn in deze scriptie verder niet toepassen. Er speelt nog een tweede factor mee bij die keuze. De wetgever heeft in het voorstel van een nieuwe verordening, die Richtlijn 2002/58/EG moet vervangen en die bij het Europese parlement

[7] In paragraaf 4.1.3 legde ik uit dat de partijen van de coalitie allemaal verwerkingsverantwoordelijken zijn.

ligt, geen beveiligingsverplichting opgenomen.[8] Als die verordening wordt aangenomen zou art. 4 van de genoemde richtlijn daarom komen te vervallen. Anticiperend op deze verordening, en gelet op het feit dat de wetgever met deze verordening de verhouding tussen de Avg en Richtlijn 2002/58/EG oplost, zal ik de richtlijn dus verder niet toepassen. Het doel van de Europese Commissie is ook om de nieuwe verordening per 25 mei 2018 (tegelijk met de Algemene verordening gegevensbescherming) van toepassing te laten zijn.[17, p. 70]

Al met al kom ik dus op de volgende bepalingen van de Avg, waar plichten in staan gecodificeerd:

- Art. 32 Avg betreffende de beveiliging van persoonsgegevens
- Art. 25 Avg over gegevensbescherming door ontwerp en standaardinstellingen

4.3 De omvang van de plichten uit de Avg

In deze paragraaf beschrijf ik de omvang van de plichten gevonden in de vorige paragraaf. Dat doe ik door de overeenkomsten en de verschillen tussen beide plichten te beschrijven. Beide plichten lijken op het eerste oog namelijk redelijk verwant. Die verwantschap beschrijf ik in paragraaf 4.3.1.

Het begin van Art. 32 lid 1 Avg luidt als volgt:

> "Rekening houdend met de *stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen*, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: [...]"

Art. 25 lid 1 Avg luidt als volgt:

[8] Verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie).

> "Rekening houdend met *de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden*, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen."

Uit de hiervoor gegeven citaten wordt duidelijk dat beide plichten uit de Avg verplichten tot het nemen van (technische en organisatorische) maatregelen. Zij behelzen dus een verplichting om te doen. Uit het gearceerde deel in beide citaten blijkt dat beide plichten gecodificeerd in deze artikelen dezelfde criteria hebben om te beoordelen welke maatregelen moeten worden genomen: *de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden.*

Beide plichten hebben echter een *verschillend doel*, te beginnen met de plicht uit art. 32 Avg. Uit overweging 83 bij de Avg blijkt dat de wetgever met art. 32 Avg voor ogen heeft gehad de veiligheid te waarborgen en te voorkomen dat de verwerking inbreuk maakt op de Verordening. Uit overweging 78 bij de Avg blijkt dat de wetgever met de plicht uit art. 25 Avg voor ogen heeft om de verwerkingsverantwoordelijke te laten voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen. De door de wetgever genoemde beginselen zijn tot op heden niet gecodificeerd in het EU-recht of in nationaal recht.[11, p. 149] Het beginsel van gegevensbescherming door ontwerp vereist de implementatie van privacywaarborgen zelfs in de ontwikkel- en productiefase van een product. Het beginsel van gegevensbescherming door standaardinstellingen vereist een systematische aanpak, zodat de gebruiker een aantal privacyinstellingen krijgt.[11, p. 150] De wetgever heeft kort samengevat met art. 25 Avg het doel om al vóór het beginnen met de verwerking, tijdens de ontwikkel- en productiefase, maatregelen te laten nemen door de verwerkingsverantwoordelijke.

Er bestaat nog een verschil tussen art. 25 en 32 Avg. Art. 25 Avg vereist,

gelet op de eerder gegeven citaten van artt. 25 en 32, maatregelen met het oog op het waarborgen van *gegevensbeschermingsbeginselen*, terwijl art. 32 Avg op het risico afgestemde maatregelen vereist en voorbeelden van die maatregelen specifiek noemt in de subs van artikel 1 (niet opgenomen in het eerder gegeven citaat). Die gegevensbeschermingsbeginselen zijn vastgelegd in art. 5 Avg.

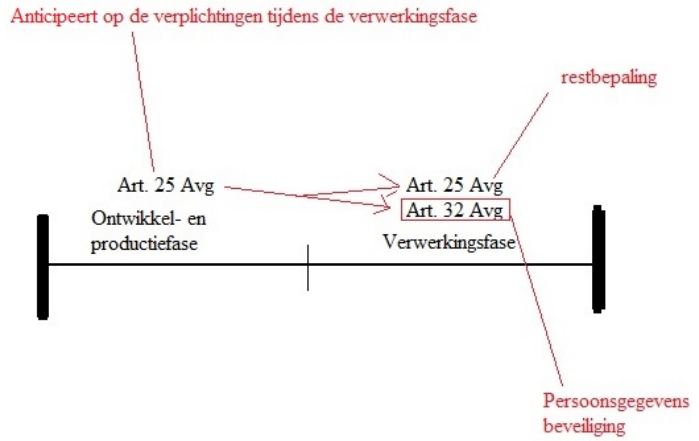
4.3.1 De samenloop tussen de plichten uit de Avg

Art. 25 en 32 Avg lijken te overlappen op het punt van versleuteling. Uit art. 25 lid 1 juncto 5 lid 1 sub f vloeit de plicht voort dat persoonsgegevens *door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.* Daaronder valt de verplichting tot versleuteling, die ook blijkt uit art. 32 lid 1 (sub a) jo. 5 lid 1 sub f Avg. Die verplichting is in het geval van het protocol relevant, omdat het protocol beslissingen neemt omtrent de versleuteling van persoonsgegevens. Dat blijkt uit het vorige hoofdstuk.

Uit de plaats van beide bepalingen valt af te leiden dat art. 32 Avg specifieker is dan art. 25 Avg. Art. 32 Avg staat immers in de afdeling getiteld "Persoonsgegevensbeveiliging", art. 25 Avg in de afdeling getiteld "Algemene bepalingen". Nergens anders heb ik de verhouding tussen beide artikelen kunnen vinden, en daarom is de *specialiteitsregel* van toepassing. De specialiteitsregel betekent dat de meer bijzondere regeling voorrang heeft boven de algemene, als in een bepaald onderwerp in twee wettelijke regelingen van gelijke rangorde op afwijkende wijze is voorzien.[16, p. 79] In het geval van artt. 25 en 32 Avg gaan beide artikelen deels over hetzelfde onderwerp. De specifieke bepaling, art. 32 Avg, heeft dus *voorrang*, voor zover dat artikel hetzelfde geval regelt als art. 25 Avg.

De figuur 4.3.1 illustreert de verhouding tussen beide hier besproken artikelen in detail, door per fase te noemen welke artikelen van toepassing zijn. Art. 25 Avg is van toepassing in zowel de ontwikkel- en productiefase als de verwerkingsfase, art. 32 Avg is slechts van toepassing in de verwerkingsfase. In de verwerkingsfase heeft art. 32 Avg wat betreft de verplichting tot bescherming van persoonsgegevens betreft dus voorrang boven art. 25. Let bovendien op het doel van art. 25 Avg dat ik beschreef in de vorige paragraaf: het doel om al vóór het beginnen met de verwerking, tijdens de ontwikkel- en productiefase, maatregelen te laten nemen door de verwerkingsverantwoordelijke. Ik concludeer daaruit dat de wetgever voor ogen heeft dat de verwerkingsverantwoordelijke wat persoonsgegevensbeveiliging betreft tij-

dens de ontwikkel- en productiefase *alvast maatregelen neemt met het oog op art. 32 Avg.* Deze interpretatie lijkt het meest aan te sluiten op de eerder beschreven bedoeling van de wetgever. Een voorbeeld van deze toepassing. Stel dat in de verwerkingsfase de verplichting tot het versleutelen van een link bestaat. Tijdens de eerdere ontwikkel- en productiefase kan op het bestaan van die verplichting al worden geanticipeert door *in het plan* voor ontwikkeling van het product alvast op te nemen dat die versleuteling plaats zal gaan vinden. Het daadwerkelijk inbouwen van versleuteling in het systeem vindt dan mogelijk later plaats, bijvoorbeeld vlak vóór de verwerkingsfase.



Figuur 4.1: De verhouding tussen de artt. 25 en 32 Avg.

4.4 Toepassing

In de hieropvolgende paragrafen zal ik telkens een of meer elementen uit artt. 25 en 32 Avg uitwerken.

4.4.1 Risico

Wat zijn de risico's die het protocol van de coalitie niet bestrijdt? Gelet op mijn conclusies in paragraaf 3.8 wordt duidelijk dat het protocol de buitenste sprongen niet beschermt. Ook kan elke mailserver tussen de verzender en de ontvanger de e-mail lezen, veranderen en vernietigen. Die mailservers kunnen groot in aantal zijn. Daardoor worden de eindgebruikers - natuurlijke personen - blootgesteld aan Confidentialityrisico's. Een voorbeeld van zo'n

risico is dat een e-mail op straat kan komen te liggen omdat die is afgeluisterd door een crimineel. Het doel van de wetgever is blijkens de tekst van artt. 32 en 25 en de daarbij horende recitals, geciteerd in paragraaf 4.3, om natuurlijke personen te beschermen tegen dit soort risico's. Het betreft immers het risico op ernstige gevolgen voor die personen: zij kunnen bijvoorbeeld reputatieschade ondervinden.

4.4.2 De aard, omvang, context en de doeleinden van de verwerking

Over de aard en de context van de verwerking van e-mails kan ik kort zijn. Bij het versturen van e-mails wordt mogelijk gevoelige informatie verzonden, waaraan de wetgever een speciale status toekent in overweging 75. Gevoelige gegevens zijn blijkens art. 9 Avg gegevens die bijvoorbeeld ras of etniciteit tot uitdrukking brengen. Zulke informatie kan worden verstuurd in een e-mail. De speciale status die de wetgever in overweging 75 toekent is dat het risico voor natuurlijke personen oploopt, met name wanneer deze gegevens worden verwerkt. In de context van e-mail in het algemeen gaat het dus om *gevoelige informatie, die goed beschermt dient te worden.*

4.4.3 De stand van de techniek

De stand van de techniek geeft end-to-endversleuteling aan als mijlpaal binnen de versleuteling van e-mailberichten, zo blijkt onder meer uit een onderzoeksrapport van ENISA.[1, p. 28] End-to-endversleuteling is de versleuteling waarbij alleen de gebruiker de e-mail kan inzien, en niet de serviceprovider of tussenliggende mailservers. Die versleuteling wordt door het protocol niet toegepast. Het protocol versleutelt namelijk slechts de binnenste sprongen, zoals blijkt uit hoofdstuk 3.8. Het protocol voldoet in dat opzicht daarom niet aan de stand van de techniek.

4.4.4 De uitvoeringskosten

De uitvoeringskosten om bijvoorbeeld de buitenste sprongen te versleutelen zouden moeten meevallen. Het afdwingen van die versleuteling is namelijk een optie die kan worden aangezet op de mailserver van de provider. Hoge uitvoeringskosten zijn daarom geen reden om niet de versleuteling van de buitenste sprongen af te dwingen.

4.5 Conclusie

4.5.1 Afweging

Art. 32 lid 2 Avg geeft aan dat het element *risico* het zwaarst weegt bij toepassing van de plicht tot bescherming van persoonsgegevens. Gelet op het bepaalde in de vorige paragrafen is niet voldaan aan die plicht. Ten eerste vloeit uit de plicht tot bescherming van persoonsgegevens de verplichting tot het versleutelen van de buitenste sprongen voort. Dat komt omdat het element risico het zwaarst weegt, en ik heb dat element in de paragraaf 4.4.1 zwaar ingeschat. Ook gaat het bij e-mails om gevoelige informatie. Aan de stand van de techniek is niet voldaan. De uitvoeringskosten van het nemen van maatregelen die de eindgebruiker - als natuurlijk persoon - beter beschermen lijken bovendien mee te vallen.

4.5.2 Conclusie

Al met al kom ik gelet op de vorige subparagraaf tot de conclusie dat waarschijnlijk niet is voldaan aan de plicht tot bescherming van persoonsgegevens. Daarmee is, gelet op de samenloop die ik beschreef in paragraaf 4.3.1, ook niet voldaan aan de Privacy by design-plicht. De Coalitie had in haar plannen kunnen opnemen dat de buitenste sprongen zouden worden versleuteld en zo, anticiperend op de plicht tot bescherming van persoonsgegevens, kunnen voldoen aan de Privacy By Design-plicht. Later, wanneer de verwerkingsfase eraan komt, zou de Coalitie dan de versleuteling daadwerkelijk kunnen aanzetten, zoals de plicht tot bescherming van persoonsgegevens vereist. Meer jurisprudentie is echter vereist om buiten kijf te stellen dat niet aan de in deze scriptie besproken plichten is voldaan door de partijen van de Coalitie.

Hoofdstuk 5

Verwant werk

Het meest recente en complete werk over de veiligheid van e-mailprotocollen dat ik heb kunnen vinden is het onderzoek van het Amerikaanse NIST.[13] In dat werk geeft het NIST een kort overzicht van de in deze scriptie besproken standaarden en hun eigenschappen.

Het meest recente werk in de richting van de plichten uit de Avg lijkt het paper van Wolters te zijn.[18]

Het onderzoek dat het meest lijkt op deze scriptie is het onderzoek gedaan door Gutwirth.[5] Dat onderzoek analyseert een e-mailprotocol aan de hand van inmiddels verouderd gegevensbeschermingsrecht. De plichten uit de Avg worden er namelijk niet in behandeld.

Hoofdstuk 6

Conclusies

In de inleiding stelde ik de centrale vraag van deze scriptie. Die vraag luidt: *welke voor de coalitie relevante plichten vloeien voort uit de bepalingen van de Algemene verordening gegevensbescherming, en in hoeverre voldoen de partijen in de coalitie aan die plichten door het protocol te implementeren?* Eerst zal een samenvatting worden gegeven van de conclusies die leiden tot het antwoord op die vraag, om vervolgens het antwoord te formuleren in paragraaf 6.3.

Om te weten of de partijen van de coalitie voldoen aan plichten uit de Avg met de invoering van het protocol, moest ik eerst weten hoe veilig het protocol is. Daarom heb ik in hoofdstuk 3 uitgewerkt aan welke van de securitydoelen Confidentiality, Integrity en Authentication het protocol voldoet.

6.1 Securitydoelen: samenvatting

Het protocol van de coalitie bestaat uit de standaarden STARTTLS, DNSSEC, DANE, SPF, DMARC en DKIM. Ik zal de door die standaarden bereikte securitydoelen hieronder stuk voor stuk uitwerken.

In paragraaf 3.2.2 kwam ik tot de conclusie dat STARTTLS het doel van Confidentiality op zichzelf bereikt. STARTLS zorgt voor asymmentrische versleuteling, die op zichzelf moeilijk te breken is. Daardoor worden een bericht versleuteld tussen twee partijen, en dat garandeert Confidentiality tussen die twee partijen. Toch kom ik in paragraaf 3.2.2 ook tot de conclusie dat of STARTTLS zorgt voor Confidentiality van e-mailberichten afhangt van de vraag hoe gebruik wordt gemaakt van de door STARTTLS gecreëerde versleuteling. STARTTLS wordt namelijk voor e-mail niet gebruikt tussen de eindgebruikers, maar slechts op de binnenste sprongen. Slechts binnenste sprong-Confidentiality wordt dus bereikt. Daarnaast creëert STARTTLS een

beveiligde "tunnel" waar berichten door worden verzonden. Die tunnel zorgt voor binnenste sprong-Integrity. De buitenste sprongen zijn niet beschermd door STARTTLS en ook de mailservers zelf kunnen de mailberichten veranderen.

In paragraaf 3.3.2 kom ik tot de conclusie dat DNSSEC niet meer doet dan het beveiligen van DNS. DNS zorgt ervoor dat de ontvangende mailserver kan worden gevonden. Daarom kom ik in paragraaf 3.3.2 tot de conclusie dat DNSSEC ervoor zorgt dat de ontvangende mailserver of eindgebruiker niet kan worden gewijzigd. DNSSEC zorgt dus voor Integrity van de ontvanger.

In paragraaf 3.4.1 concludeer ik, net als hierboven, dat DANE gebruik maakt van STARTTLS. DANE heeft blijkens hetgeen ik in paragraaf 3.4.2 heb beredeneerd tot doel om te zorgen voor Confidentiality. DANE zorgt echter, net als STARTTLS, slechts voor binnenste sprongversleuteling. De verbinding in de buitenste sprongen worden door DANE niet versleuteld. Bovendien kunnen alle mailservers in de binnenste sprongen de e-mailberichten ook bij het gebruik van DANE nog lezen. DANE zorgt daarnaast voor ontvangende mail server Authentication, aangezien het de publieke sleutel van de ontvangende mailserver controleert voordat het toestaat dat een mail naar die server gestuurd wordt. In paragraaf 3.5.1 beschrijf ik de werking van SPF. Op basis van die werking kom ik in paragraaf 3.5.2 tot de conclusie dat SPF zorgt voor domain Authentication van de verzender. SPF gebruikt het bron IP-adres uit de "FROM"header van de ontvangen e-mail om te kijken of het domein van de verzender toestaat dat dat IP-adres een e-mail verstuurt.

In paragraaf 3.6.2 stel ik vast dat DKIM zorgt voor Integrity in de binnenste sprongen. DKIM controleert de digitale handtekening in mailberichten met behulp van een DNS record.

In paragraaf 3.7.2 concludeer ik dat DMARC niet meer doet dan SPF en DKIM samen. Het stuurt wel nuttige rapporten, maar dat verandert niets aan de securitydoelen die het protocol behaalt.

Op basis van het voorgaande kom ik uit op tabel 3.1, die hieronder opnieuw gegeven is.

	STARTTLS	**DNSSEC**	**DANE**	**DMARC**	
				SPF	**DKIM**
Bereikte securitydoelen	• Binnenste sprong Confidentiality • Binnenste sprong Integrity	Integrity van de bestemming	• Binnenste sprong Confidentiality • Binnenste sprong Integrity • Binnenste sprong ontvangende mail server Authentication	Domain Authentication van de verzender	Integrity tussen versturende mail provider en ontvanger in de binnenste sprongen

Op basis van de tabel hierboven concludeer ik dat het protocol geen van

de securitydoelen Confidentiality, Authentication en Integrity bereikt. Dat komt omdat de mailservers tussen de serviceproviders e-mails kunnen onderscheppen, lezen en veranderen. Ook worden de drie benoemde doelen niet bereikt omdat op de buitenste sprongen geen versleuteling wordt afgedwongen. Daardoor kan de volledige inhoud van e-mailberichten door kwaadwillende derden worden onderschept, gelezen en veranderd.

6.2 Plichten uit de Avg: samenvatting

In paragraaf 4.1 concludeerde ik dat de Verordening van toepassing is op de coalitie. In paragraaf 4.2 leidde ik twee voor de coalitie relevante plichten uit respectievelijk art. 32 en 25 Avg. Beide plichten brengen verplichtingen voort tot het nemen van technische en organisatorische maatregelen. In paragraaf 4.3 concludeerde ik ten eerste dat het een verplichting tot een doen betreft, er moeten immers maatregelen worden genomen. Bovendien hangt het van een aantal criteria af welke concrete verplichtingen voortvloeien uit de eerder genoemde plichten. Die criteria zijn de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. Bij de toepassing van de plicht uit art. 32 Avg weegt het element risico bovendien het zwaarst, zo blijkt uit art. 32 lid 2 Avg. Het doel daarvan is de bescherming van natuurlijke personen tegen de risico's die samenhangen van de verwerking.

Bovendien is er nog een derde mogelijke plicht, die ik in de scriptie niet toepas. Volgens art. 95 Avg geldt de Avg niet voor zover plichten uit de Avg op grond van Richtlijn 2002/58/EG onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling. In art. 4 van die richtlijn staat in verhouding tot art. 32 Avg een soortgelijke plicht beschreven met dezelfde doelstelling. Ik concludeer echter dat art. 95 Avg slechts een tijdelijke maatregel beoogt te bewerkstelligen en dat de commissie van plan is om art. 4 van de eerder genoemde richtlijn te schrappen met een nieuwe verordening die gelijktijdig met de Avg van kracht wordt. Daarom leid ik slechts uit artt. 25 en 32 Avg relevante plichten af, die na paragraaf 4.3 worden toegepast.

In paragraaf 4.4 pas ik de plichten uit artt. 25 en 32 Avg toe. Uit mijn conclusies van hoofdstuk 3 leid ik af dat de risico's voor natuurlijke personen (zoals de eindgebruiker) erg groot zijn. Het feit dat de buitenste sprongen niet versleuteld zijn betekent dat er een kans bestaat dat kwaadwillende derden de e-mails onderscheppen, veranderen en lezen. Bovendien kunnen kwaadwillenden de mailservers tussen providers overnemen. Ook in dat geval kunnen zij alle e-mails veranderen en lezen. Ten tweede leid ik uit de visie

van de wetgever af dat er een indicatie voor hoge risico's is als er veel gevoelige informatie wordt verstuurd. Bij e-mail wordt mogelijk veel gevoelige informatie verstuurd, dus ook volgens de visie van de wetgever lijkt een hoge risicoinschatting duidelijk. E-mails bevatten gevoelige informatie, en in die context zijn de verplichtingen tot versleuteling ervan zwaar. Ook dat moeten worden meegewogen. In paragraaf 3.4 concludeer ik bovendien dat het budget moet worden meegerekend. Als het bijvoorbeeld te veel zou kosten om de buitenste sprongen te beveiligen, dan zou dat een reden zijn waarom de verplichting tot versleuteling lichter is. Echter gaat het in dit geval om een optie die eenvoudig kan worden aangezet om versleuteling met de buitenste sprongen af te dwingen. Daarom schat ik de kosten laag in. Daarom is niet voldaan aan de plicht uit art. 32 Avg. Bovendien kunnen providers meer doen dan alleen de binnenste sprongen versleutelen om veilig e-mails uit te wisselen met andere providers. Op zijn minst kunnen zij met een optie de buitenste sprongversleuteling afdwingen, om op die manier de Confidentiality risico's op die servers te verkleinen. Daarom is niet voldaan aan de plichten uit art. 32 en 25 Avg.

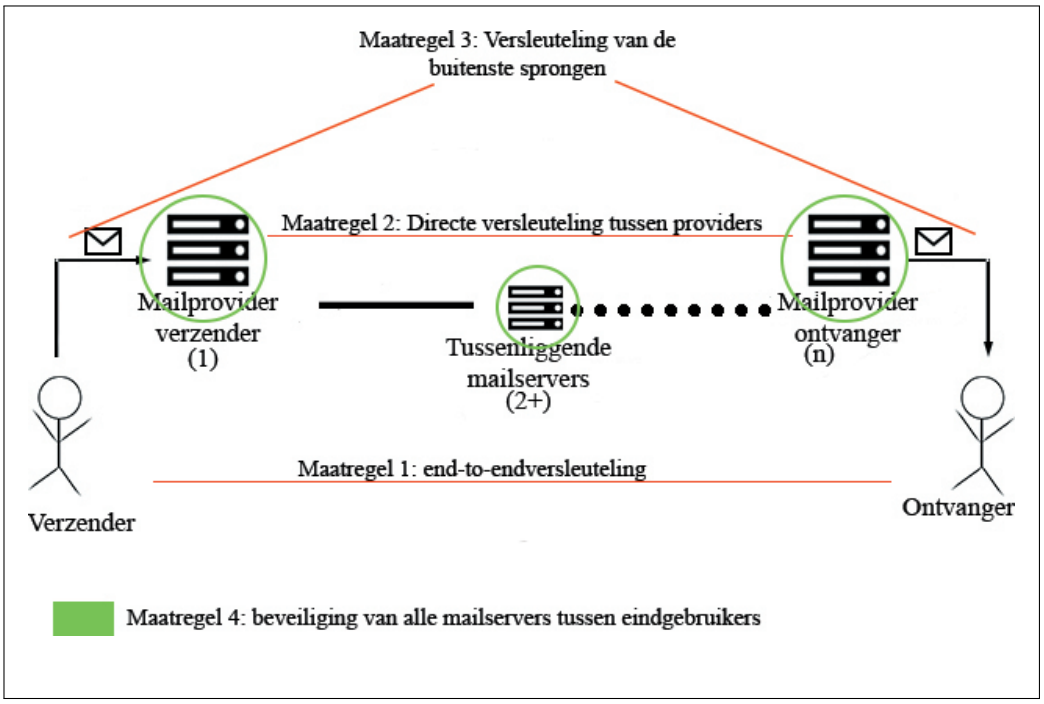
6.3 Conclusie

Al met al kom ik tot de conclusie dat niet is voldaan aan de plichten uit de Avg met de invoering van het protocol. Eindgebruikers worden door het protocol onvoldoende beschermd tegen de gevolgen van Confidentialityinbreuken, gevolgen waartegen de Avg hen als natuurlijke personen nu juist beoogt te beschermen.

6.4 Discussie

In de vorige paragraaf sloot ik af met de conclusie dat de eindgebruiker, ondanks invoering van het protocol, mogelijk wordt blootgesteld aan onaanvaardbare risico's. In deze paragraaf zal ik een viertal technische maatregelen noemen die de eindgebruiker kunnen beschermen tegen die risico's. De eerste maatregel komt neer op het end-to-end versleutelen van e-mails tussen eindgebruikers. De tweede maatregel komt neer op het versleutelen van de buitenste sprongen. De derde maatregel is het direct versleutelen van e-mails tussen mailproviders. De laatste maatregel komt neer op het verzekeren van de veiligheid van de tussenliggende servers. Ik zal deze vier oplossingen hierna achtereenvolgens uitwerken. De figuur op de volgende pagina geeft alle maatregelen grafisch weer. De rode lijnen en groene cirkels geven de

mogelijke maatregelen aan.



De eerste mogelijke maatregel is het end-to-endversleutelen van e-mails tussen de eindgebruikers. Bij end-to-endversleuteling kunnen slechts de eindgebruikers de e-mail lezen. Er bestaan een aantal protocollen, zoals OpenPGP, die dit mogelijk maken. De bruikbaarheid voor de eindgebruiker is bij die protocollen echter een heikel punt. De eindgebruiker moet een aantal handelingen verrichten, zoals het aanmaken, publiceren en uitwisselen van (publieke) sleutels, om end-to-endversleuteling in te stellen. Uit empyrische studies blijkt echter dat die stappen voor de gemiddelde gebruiker te veel moeite en te complex zijn. De gemiddelde eindgebruiker heeft voor het nemen van die stappen namelijk een gebrek aan technische kunde.[9] Een e-mailstandaard die geen extra handelingen door de eindgebruiker vereist ben ik bovendien niet tegengekomen.

[9] Zie het paper van Payne en Edwards over het gebrek van bruikbaarheid van end-to-endstandaarden voor e-mail. Uit empyrische studies blijkt volgens hen dat gebruikers vaak een zwak wachtwoord kiezen en geheime sleutels onversleuteld naar elkaar e-mailen. B. D. Payne en W. K. Edwards, "A brief introduction to usable security", *IEEE Internet Computing*, vol. 12, nr. 3, p. 15-16, 2008. Zie bijvoorbeeld het paper van Lampson over het belang van en de discussie over bruikbare cyberbeveiliging. B. Lampson, "Privacy and security. Usable security: how to get it", *Communications of the ACM*, vol. 52, nr. 11, p. 25, nov. 2009.

De tweede maatregel lijkt mij het versleutelen van de buitenste sprongen. Daardoor kunnen e-mails niet meer worden onderschept of gelezen op die sprongen. Het afdwingen van deze versleuteling kan eenvoudig middels één enkele optie binnen SMTP.

Een derde maatregel is het versleutelen van de e-mail tussen de providers met behulp van bijvoorbeeld public key-versleuteling. Hiermee bedoel ik niet de versleuteling van de binnenste sprongen, maar directe versleuteling tussen providers. De ene mailprovider zal de e-mail dus versleutelen en de andere mailprovider zal hem ontsleutelen. Tussenliggende mailservers kunnen de ontsleutelde inhoud van de e-mail dan niet lezen. Om de hier beschreven maatregel mogelijk te maken zouden afspraken tussen mailproviders gemaakt moeten worden, of er zou een uniforme standaard bedacht moeten worden.

De laatste maatregel die ik kan bedenken is het verzekeren van de beveiliging van de mailservers. Dat kan door middel van een contractueel beding met een derde zijn, maar ook door het beter beveiligen van de servers door middel van updates die zwakheden oplossen of door middel van een firewall. Een contractueel beding zou bijvoorbeeld gebruikt worden als de server onder het beheer van een derde staat.

De Avg vereist slechts de behandeling van de risico's. De minimale combinatie van de hierboven beschreven maatregelen die de Avg vereist lijkt mij daarom de versleuteling van de buitenste sprongen, en het beschermen van elke server tussen de eindgebruikers. Dat is een combinatie van de tweede en de vierde maatregel die eerder genoemd zijn. De risico's vloeien immers voort uit het ontbreken van maatregelen die versleuteling afdwingen en servers beveiligen.

Van de vier uitgewerkte oplossingen lijkt mij een combinatie van de tweede en de derde, directe versleuteling tussen mailproviders en versleuteling van de sprong tussen mailprovider en eindgebruiker, het meest geschikt. Ik zal nu twee argumenten voor en één argument tegen de keuze voor die oplossing uitwerken, en het tegenargument ontkrachten.

Het eerste argument vloeit voort uit de instemming die en het vertrouwen dat de eindgebruiker heeft gegeven aan de mailprovider. De eindgebruiker is zich ervan bewust en staat toe dat de e-mail wordt opgeslagen op de server van de mailprovider. De eindgebruiker vertrouwt er daarom op dat de mailprovider diens mailserver afdoende beveiligt. De eindgebruiker heeft echter geen vertrouwen in de mailservers tussen de providers, de tussenliggende mailservers. Het lijkt mij dus noodzakelijk voor de mailprovider om meer te doen dan slechts de maatregelen te nemen die de verordening vereist. De eindgebruiker aanvaard immers dat e-mails op de server van de mailprovider

kunnen worden ingezien (denk bijvoorbeeld aan webmail), maar hij heeft er niet bewust mee ingestemd dat beheerders van andere e-mailservers de e-mails in principe ook kunnen inzien. Als een e-mail bijvoorbeeld "op straat komt te liggen" omdat een tussenliggende mailserver onvoldoende is beveiligd, dan kan dat bovendien voor grote maatschappelijke ophef zorgen. De eindgebruiker vertrouwt er immers op dat de mailprovider geen toestemming aan derden geeft om de e-mails te beheren en in te zien, terwijl de mailprovider die toestemming in werkelijkheid mogelijk wel geeft.

Het tweede argument komt erop neer dat de provider met deze oplossing meer grip heeft over het al dan niet uitlekken van e-mails. Een mailprovider beheert zijn eigen mailservers vaak zelf, maar niet de mailservers van derden. Door e-mails tussen providers te versleutelen krijgen deze providers in ieder geval de mogelijkheid om zelf alle concrete maatregelen over de beveiliging te nemen.

Een tegenargument gaat over de verdeling van verantwoordelijkheid binnen de eerder gekozen combinatie van maatregelen. De verzendende mailprovider moet volgens die combinatie zélf de e-mails versleutelen, in ieder geval tot de ontvangende mailprovider. De ontvangende mailprovider moet vervolgens de e-mail versleuteld naar de ontvanger versturen. De gekozen combinatie van maatregelen legt daarom veel verantwoordelijkheid bij de mailproviders, terwijl de beveiliging van de e-mails binnen de Avg een gedeelde verantwoordelijkheid is.[10] De mailprovider mag immers op derden vertrouwen om tussenliggende mailservers te beheren, hij moet zich er slechts van verzekeren dat de derden de e-mails goed bezorgen.

Het bovenstaande tegenargument miskent echter het feit dat de mailprovider juist degene is die het gehele proces van verzenden en ontvangen van de e-mails goed kan beveiligen. De mailprovider heeft in dat opzicht meer grip over de beveiliging dan derden waarmee hij een overeenkomst sluit. Daarom lijkt het mij juist gepast dat hij meer doet dan voldoen aan de eerder uitgewerkte minimale eisen van de Avg.

6.5 Suggestie ter verbetering

De eindgebruiker heeft vertrouwen in de provider, en daarom mogen e-mails wat de eindgebruiker betreft waarschijnlijk bewaard worden op diens server. Bovendien kan de mailprovider meer grip krijgen over confidentialityrisico's als hij zelf meer verantwoordelijkheid neemt. Een tegenargument is dat de

[10] Zie bijvoorbeeld het paper van Wolters waarin hij door middel van een casus aantoont dat de verplichting tot beveiliging van persoonsgegevens binnen het stelsel van de Avg een gedeelde verantwoordelijkheid meebrengt.[18, p. 145]

mailprovider in dat geval vrijwel alle verantwoordelijkheid voor het nemen van maatregelen krijgt. Daar kan tegen in worden gebracht dat de provider de ideale positie heeft om e-mails beter te beveiligen, en daardoor die verantwoordelijkheid op zich zou moeten nemen. Bovendien weegt het argument van instemming van de eindgebruiker naar mijn mening zwaarder dan het eerder uitgewerkte tegenargument. Het is mijns inziens namelijk belangrijker dat het vertrouwen van de eindgebruiker niet wordt geschaadt, dan dat de verantwoordelijkheden over de beveiliging van de e-mails evenredig worden verdeeld. Een bijpassend voordeel is dat de mailprovider meer grip krijgt over de risico's, omdat de gehele versleuteling tot de ontvangende mailprovider in zijn macht komt te liggen.

Gelet op het bovenstaande is mijn suggestie de combinatie van *het direct versleutelen van e-mails tussen mailproviders* en *het versleutelen van de buitenste sprongen*. Dat is een combinatie van de tweede en derde maatregel die ik eerder uitwerkte. E-mail zou door die combinatie van maatregelen te nemen een stuk veiliger zijn, terwijl rekening wordt gehouden met de technische vaardigheden van de eindgebruiker en de mate van instemming die hij geeft tijdens het versturen van een e-mail.

Bibliografie

[1] Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, George Danezis, European Union, and European Network and Information Security Agency. *Privacy and data protection by design - from policy to engineering.* ENISA, Heraklion, 2014. OCLC: 903502987.

[2] Amy Friedlander, Allison Mankin, W. Douglas Maughan, and Stephen D. Crocker. DNSSEC: A Protocol Toward Securing the Internet Infrastructure. *Commun. ACM*, 50(6):44–50, June 2007.

[3] Joseph Gersch, Dan Massey, and Scott Rose. DANE Trusted Email for Supply Chain Management. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[4] Michael Goodrich and Roberto Tamassia. *Introduction to Computer Security.* Addison-Wesley Publishing Company, 2010.

[5] Serge Gutwirth. *Reforming European data protection law.* Issues in privacy and data protection, 2352-1929 volume 20.; Law, governance and technology series ; 2352-1902 v. 20.; Issues in privacy and data protection. 2352-1929. Springer,, Dordrecht :, 2015.

[6] Amir Herzberg and Haya Shulman. Towards Adoption of DNSSEC: Availability and Security Challenges. *IACR Cryptology ePrint Archive*, 2013:254, 2013.

[7] P. Hoffman. SMTP Service Extension for Secure SMTP over Transport Layer Security. Technical Report RFC3207, RFC Editor, February 2002. DOI: 10.17487/rfc3207.

[8] Ralph Holz, Yaron Sheffer, and Peter Saint-Andre. Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS), February 2015.

[9] J. Klensin. Simple Mail Transfer Protocol. 2008.

[10] Hugo Krawczyk, Kenneth G. Paterson, and Hoeteck Wee. On the Security of the TLS Protocol: A Systematic Analysis. In *Advances in Cryptology – CRYPTO 2013*, pages 429–448. Springer, Berlin, Heidelberg, 2013. DOI: 10.1007/978-3-642-40041-4_24.

[11] Mariusz Krzysztofek. *Post-reform personal data protection in the European Union. General data protection regulation (EU) 2016/679*. Wolters Kluwer, Alphen aan den Rijn, 2017.

[12] Jim Kurose and Keith Ross. Computer Networking. A Top Down Approach 6th Edition. 2012.

[13] Scott W. Rose, Stephen J. Nightingale, Simson L. Garfinkel, and Ramaswamy Chandramouli. Trustworthy Email. Technical Report NIST SP 800-177, National Institute of Standards and Technology, September 2016. DOI: 10.6028/NIST.SP.800-177.

[14] P.J. Slot, R. Barents, and Rick Lawson. *Inleiding Europees recht*. Wolters-Noordhoff, Groningen, 2005.

[15] Pawel Szalachowski and Adrian Perrig. Short Paper: On Deployment of DNS-based Security Enhancements. *arXiv preprint arXiv:1702.05311*, 2017.

[16] J. W. P. Verheugt. *Inleiding in het Nederlandse recht*. Boom juridische studieboeken. Boom Juridische uitgevers, Den Haag, 17e [geactualiseerde] dr. edition, 2013.

[17] M.A.M. Verveld-Suijkerbuijk. Het Europese voorstel voor een e-Privacyverordening. *Privacy & Informatie*, 2(58), April 2017.

[18] P.T.J. Wolters. De beveiliging van persoonsgegevens. Een geharmoniseerde verplichting of een gedeelde verantwoordelijkheid? *Tijdschrift voor Europees en economisch recht*, 2017(1):144–157, April 2017.

[19] Meng Weng Wong. SPF Overview. *Linux J.*, 2004(120):2, April 2004.