Veilig omgaan met e-mail in de zorg

INFORMATIEBEVEILIGING

Betere zorg
door betere informatie

Nictiz

Datum	ID Nummer		
7 januari 2015	1		

Auteurs
Jan Jongenelen
Maarten Ligtvoet

Samenvatting
In de context van de bescherming van de privacy neemt de belangstelling voor veilige e-mail toe. Veel instellingen in de zorg staan op het punt om een aanpak te kiezen. Er zijn verschillende methoden om e-mail te beveiligen, met verschillende aanbieders. Welke oplossing men kiest moet afhankelijk zijn van een risico-analyse.
Beveiligingsproducten concentreren zich veelal op de bescherming van informatie tijdens het transport. Terwijl de kwetsbaarheid van informatie aanwezig op de werkplek misschien wel groter is. Beschouw veilige e-mail daarom als een onderdeel van informatiebeveiliging en niet als een opzichzelfstaand vraagstuk.
Dit document beschrijft de risico's en de kwetsbaarheden van e-mail, en houdt verschillende oplossingen tegen het licht.

Inhoud

1 Inleiding

In welke mate zorgverleners gebruikmaken van onbeveiligde e-mail is niet bekend. Dat het gebeurt is wel zeker. Tot nog toe maakten vooral security-officers in de zorg zich ongerust over het uitwisselen van privacygevoelige medische gegevens via e-mail. Inmiddels dringt de ongerustheid ook door in de media (Reijnoudt) [1]. Veel instellingen worden zich bewust van de imagoschade en omzetdaling die het gevolg kan zijn van incidenten in de informatiebeveiliging en overwegen een oplossing voor veilige e-mail te selecteren. Waaruit kunnen ze kiezen? Waarop moeten ze letten? Het antwoord op deze vragen kan men vinden in deze publicatie. De publicatie geeft inzicht in de actuele mogelijkheden en de toegepaste technieken; de voor- en nadelen van verschillende architecturen voor veilige e-mail; en een visie op de toekomst van e-mail in de zorg.

Informatiebeveiliging kent drie pijlers: vertrouwelijkheid, integriteit en beschikbaarheid. Bescherming van de vertrouwelijkheid is het eerste waar men aan denkt bij veilige e-mail. Vooral dit aspect belichten wij in dit document. Daarnaast geven we aandacht aan authenticatie: de zekerheid dat degene aan de andere kant van de lijn is voor wie hij zich uitgeeft.

Absoluut 'veilig' of 'onveilig' is een valse tweedeling

Er is altijd een uitruil tussen vertrouwelijkheid en werkbaarheid[2]. Het hoogste niveau van bescherming leidt tot een grotendeels inert bedrijf. Het veiligste systeem is dat waar geen informatie wordt uitgewisseld. Gegevens moeten niet alleen vertrouwelijk zijn en integer, maar ze moeten ook beschikbaar zijn voor de mensen die met informatie moeten werken. Zeker in de zorg, waar veel mensen betrokken kunnen zijn bij de behandeling van een patiënt, is het een uitdaging om aan beschikbaarheid en vertrouwelijkheid te voldoen.

Scope

Waarom hebben we het alleen over veilige e-mail? Want waarom zouden we het alleen hebben over veiligheid van informatie in transit? Het moet natuurlijk gaan om beveiliging van informatie in het algemeen. Deze verkenning behandelt veilige e-mail, met de kanttekening dat dit onderwerp gezien moet worden als een onderdeel van informatiebeveiliging in brede zin.

1.1 Doelgroep

Deze verkenning is bedoeld voor managers ICT in de zorg die kampen met de vraag welke techniek te gebruiken en zich afvragen of ze daarmee voldoen aan de actuele richtlijnen. Aangezien vrijwel iedereen gebruikmaakt van e-mail en er steeds meer zorgen zijn over de privacy, verwachten we dat velen interesse hebben in dit rapport. De daadwerkelijke lezers en raadplegers van het rapport zoeken wij onder de security-officers en de ICT-beslissers: de mensen die verantwoordelijk zijn voor informatiebeveiliging en die op het matje geroepen worden bij incidenten. Op die doelgroep is het rapport gericht.

1.2 Opzet

De inhoud van deze verkenning is samengesteld gebruikmakend van vele openbaar beschikbare documenten, zie de bijlage 'Geraadpleegde bronnen'. Daarnaast zijn gesprekken gevoerd met de volgende mensen:

Prof. Bart Jacobs, hoogleraar Software Security and Correctness aan de Radboud Universiteit;
Margriet Miedema, directeur en Zorgring NHN;
Dieter Vorderhake, Project Manager Stichting;
Dave Ormel, manager RSO Haaglanden;
Rob Saathof, projectmanager Sleutelnet;
Maarten Wittop Koning, innovatiedirecteur KPN Zorg;
Joris Knaapen, innovatiemanager KPN Zorg;

[1] Gevoelige-medische-dossiers-worden-vaak-illegaal-onbeveiligd-rondgemaild, de correspondent.

[2] Vooral Bruce Schneier schrijft veel over deze uitruil.

Dirk Jan Schwietert, directeur Software Connection (Voltage reseller Nederland);
Clarine ter Kuile, manager Software Connection;
Brendan Rizzo, Technical Director Voltage Security;
Joke Koops, productmanager ENOVATION
Johan Vos, productmanager ENOVATION;
Maarten Fischer, beleidsadviseur Nederlandse Vereniging van Ziekenhuizen (NVZ);
Hedde van der Lugt, manager standaarden en kwaliteit Nictiz
Johan Krijgsman, manager monitoring & TrendITion Nictiz;
Deskundigen van het NCSC[1].

De informatie uit de interviews en de bronnen hebben we verwerkt in dit rapport. Alle geïnterviewden hebben op het concept commentaar geleverd, dat zo goed mogelijk verwerkt is. Omdat iedereen net weer andere accenten legt, en omdat het eindproduct een samenstelling van verschillende visies is, reflecteert dit rapport niet integraal de mening van een van bovenstaande mensen. Het blijft de analyse van Nictiz.

De leveranciers die in dit stuk genoemd worden, bevestigen dat datgene wat over hun product geschreven staat correct is. De producten worden beschreven op hoofdlijnen; details zijn vanzelfsprekend bij hen op te vragen.

1.3 Opbouw van het document

Eerst staan we stil bij het begrip 'veilig' en analyseren we welke dreigingen er zijn en uit welke hoek inbreuken zijn te verwachten, hoofdstuk 2. Dan gaan we in op de onderliggende techniek van e-mail en bespreken de kwetsbaarheden op de weg die een e-mail aflegt van persoon naar persoon, hoofdstuk 3. Ten derde bespreken we de technieken die de kwetsbaarheden verminderen, meteen gevolgd door hun leveranciers in hoofdstuk 4. We sluiten af met conclusies en een korte blik naar de toekomst in hoofdstuk 5 en 6.

1.4 Terminologie

In dit stuk worden *versleuteling*, *vercijfering* en *encryptie* als synoniemen gebruikt. Het omgekeerde is *ontcijfering*. Er is hier en daar gepoogd Engelse termen te vervangen door Nederlandse. In plaats van *face-to-face* schrijven we bijvoorbeeld in levenden lijve. Een *device* wordt een *apparaat*. De *verzender* en *ontvanger* worden ook wel *correspondenten* genoemd. De *ontvanger* is tevens de *geadresseerde*.

[1] Het Nationaal Cyber Security Centrum (NCSC) draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief.
Het centrum valt onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het ministerie van Veiligheid en Justitie.

2 Wat is veilig?

Veiligheid is geen binair attribuut; het kent gradaties. Of een e-mail veilig is verstuurd, is niet met ja of nee te beantwoorden; alle e-mail is in zekere mate beveiligd.

Als men het heeft over beveiliging is niet volledig duidelijk welk niveau is vereist. De Wet Bescherming Persoonsgegevens(WBP) spreekt in artikel 13 over een **passende** manier van beveiligen en laat – terecht – de invulling van passendheid aan het veld.

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen."

In Richtsnoeren beveiliging persoonsgegevens (CBP, 2013) legt het CBP uit hoe de beveiliging van persoonsgegevens in individuele gevallen zou moeten worden toegepast:
"Als met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd (zal) deze als 'passend' moeten worden beschouwd, terwijl kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist."

Om passende maatregelen te nemen is het noodzakelijk de risico's in te schatten. In de volgende pagina's doen we een analyse.

2.1 Welke bronnen van dreiging zijn er?

In deze paragraaf benoemen wij uit welke hoek wij inbreuk op de vertrouwelijkheid kunnen verwachten of voorstellen. De inventarisatie is gebaseerd op het NCSC cybersecurity beeld Nederland 2014 (NCSC, 2014)

1. Populaire producten en diensten.
   De privacy staat onder druk door de populaire (gratis) producten en diensten aangeboden door bedrijven die de informatie gebruiken om geld te verdienen. In de voorwaarden van bijvoorbeeld Google staat:

   *Onze geautomatiseerde systemen analyseren uw inhoud **(inclusief e-mails)** om voor u relevante productfuncties te leveren, zoals aangepaste zoekresultaten, advertenties op maat en spam- en malwaredetectie. Deze analyse vindt plaats wanneer de inhoud wordt verzonden, ontvangen en opgeslagen.*

   Gezien de populariteit van deze producten en diensten, vinden heel veel Nederlanders dit niet erg. Maar is het acceptabel dat een zorginstelling informatie uitwisselt via bedrijven die de intentie hebben om gegevens die niet voor hun bedoeld zijn commercieel te gebruiken? In welke mate zorgaanbieders van deze diensten gebruikmaken is niet bekend, maar even googelen - met zoeksleutels als "herhaalrecept" en "gmail.com" levert al tientallen resultaten op in de trant van: herhaalrecepten@gmail.com en informatieavondovergang@gmail.com Overigens zijn niet meteen alle webmail-aanbieders in de ban. Er zijn veel - vaak betaalde - alternatieven die commercieel gebruik uitsluiten[1].

2. Overheden en hun inlichtingendiensten.
   Er is grote onbekendheid met de mogelijkheden en macht van inlichtingendiensten. De Amerikaanse National Security Agency (NSA) is een sprekend voorbeeld van een inlichtingendienst die soms negatief in het nieuws komt wegens het clandestien

[1] Zie bijv. Bits Of Freedom : https://www.bof.nl/2012/04/13/zo-vind-je-een-goed-alternatief-voor-gmail-2/

verzamelen van data (Olsthoorn, 2014). Ziekenhuisdirecties en/of burgers zouden bang kunnen zijn dat medisch inhoudelijke informatie die uiteraard erg privacy-gevoelig is, wordt onderschept door dergelijke diensten.

3. Criminelen die informatie te gelde willen maken.
   Het is onduidelijk hoe actief criminelen zijn in het hacken van medische dossiers. Met enige regelmaat wordt beweerd dat criminelen belust zouden zijn op medische data omdat die veel geld kunnen opleveren[1]. Er wordt gesproken van het chanteren van mensen. Dat is echter een vermoeden; bewijzen daarvan zijn er (nog) nauwelijks. Totdat er sterkere aanwijzingen zijn, moeten we de beweringen met een korrel zout nemen.
   Dit laat onverlet dat men zich tegen criminelen moet wapenen. Zij zijn op zoek naar gegevens die hun in staat stellen zich voor iemand anders uit te geven: identiteitsfraude. Het Cybersecuritybeeld Nederland 2014 (NCSC, 2014) waarschuwt ook voor de opkomst van ransomware. Criminelen maken gegevens onbruikbaar en vragen een losprijs om de gegevens te herstellen. Dit is een 'mooi' voorbeeld van een dreiging waarbij de beschikbaarheid in het geding is.
   In hetzelfde document wordt gewaarschuwd voor afpersing van bedrijven onder dreiging van publicatie van buitgemaakte gegevens. Het valt niet uit te sluiten dat dit in de zorg de kop opsteekt.

4. Nieuwsgierigheid van mensen in de omgeving die toevallig dingen van je te weten kunnen komen. Dit is de klassieke privacyschade die niet in geld uit te drukken is. Veel mensen vinden vooral deze inbreuk ernstig omdat het mensen van vlees en bloed zijn die de persoonlijke levenssfeer schenden. Dit in tegenstelling tot de bij 1 en 2 genoemde actoren die anoniem zijn en waar waarschijnlijk alleen slimme software de e-mail leest en analyseert.

5. Hacktivisten en/of journalisten die misstanden over bescherming van de privacy aan de kaak willen stellen. Incidenten leiden tot grote imagoschade en omzetdaling voor de nalatige organisatie.

Allen die verantwoordelijk zijn voor beveiliging van aan hen toevertrouwde gevoelige informatie, moeten zich afvragen welke dreigingen reëel zijn en tegen welke dreiging zij zich willen beschermen. Daarnaast is het raadzaam om een inschatting te maken van de kans dat inbreuken optreden en de schade daarvan.

Om de lezer niet het bos in te sturen met deze goede raad, hieronder een voorbeeld van een uitwerking.

Ad. 1 Kunnen we in de zorg diensten afnemen van bedrijven die de inhoud van e-mails willen lezen en gebruiken? Ofschoon het College Bescherming Persoonsgegevens (CBP) zich er nog niet expliciet over heeft uitgesproken, is het niet heel gewaagd te stellen dat persoonsgegevens op deze manier vatbaar worden voor *onrechtmatige verwerking* zoals bedoeld in de WBP. Omdat deze aanbieders niet illegaal handelen is de bescherming eenvoudig: ontmantel die e-mailaccounts en kies andere.

Ad. 2 Tegen de inlichtingendiensten kan men zich moeilijk verdedigen. Nederlandse inlichtingendienst kunnen gegevens met gerechtelijke bevelen opeisen. Als buitenlandse inlichtingendiensten samenwerken met de Nederlandse kunnen zij zo ook data in Nederland collecteren. Het is de vraag of een zorginstelling zich hiertegen moet beveiligen. De Nederlandse overheid kan de grenzen aangeven waarbinnen bijvoorbeeld de Nederlandse inlichtingendienst mag opereren. De zorginstelling kan zelf een risico-inventarisatie maken om dit mogelijke risico al dan niet af te dekken.

Ad. 3 Voorlopig taxeren we de kans op het optreden van criminele inbreuken als klein, gezien de

[1] http://www.telegraaf.nl/dft/nieuws_dft/22934585/__Cyberbendes_jagen_op_medische_dossiers__.html

afwezigheid van precedenten. De schade zal wel de kwalificatie ‘ernstig’ verdienen.

Ad. 4 Als het mogelijk is om de nieuwsgierigheid te bevredigen, de kans op detectie is klein en de sanctie is licht, dan is de kans groot dat dit gebeurt. Omdat deze actoren doorgaans niet over geavanceerde cybercrime software beschikken, is de manier om je te beveiligen ook niet geavanceerd technisch. Deze is gericht op procedures en bewustwording.

Ad. 5 De kans dat hacktivisten een lek zullen exploiteren, indien de gelegenheid zich voordoet, is groot. De imagoschade van de organisatie die ‘nalatig’ is geweest, is groot. Niet beschermen is geen optie.

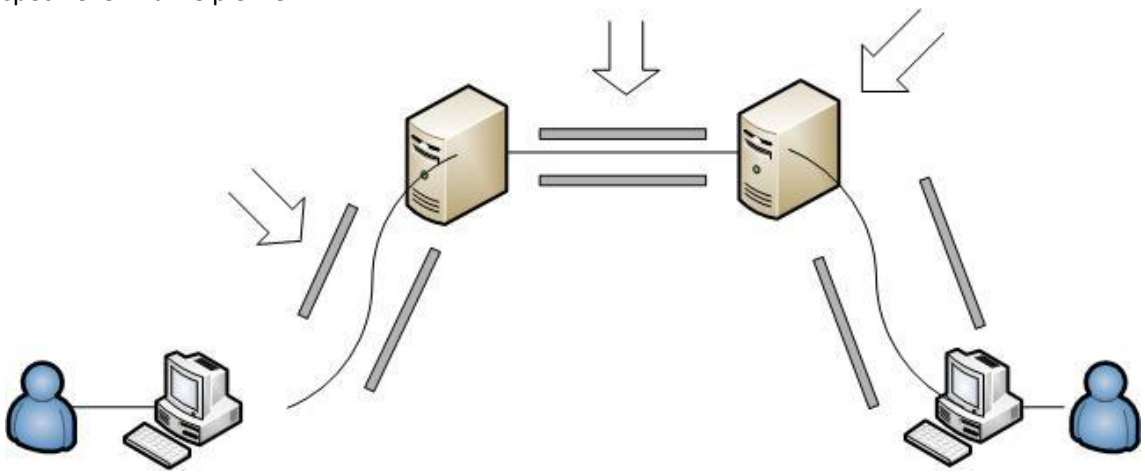
De inschatting van de risico’s is subjectief en zal als gevolg van nieuwe informatie kunnen veranderen. De verantwoordelijken voor informatiebeheer en uitwisseling dienen deze afwegingen voor hun instelling zelf te maken en te evalueren.

3 Wat zijn de zwakke plekken van e-mail?

E-mail is uitgevonden in het prille begin van internet. Het ontwerp heeft in het geheel geen rekening gehouden met beveiliging. Een e-mail is te vergelijken met een ansichtkaart die iedereen die hem door de handen gaat kan lezen of zelfs veranderen. Iedereen die een ansicht verstuurt weet dat. Gelukkig zijn er in de loop der jaren wel flankerende maatregelen genomen die de veiligheid van e-mail vergroten.

3.1 De e-mail-keten in het kort

Heel eenvoudig gezegd bestaat de e-mailketen uit: Persoon – apparaat[1]- mailserver- mailserver – apparaat – persoon. Het versturen van e-mail gaat in verschillende stappen. Elke stap heeft zijn specifieke zwakke plekken.



Figuur 1. E-mailtraject

3.2 Van persoon naar apparaat

De interactie van de eindgebruiker met zijn computer. Is het wachtwoord dat iemand kiest sterk of zwak? Hangt er een post-it met inloggegevens aan het beeldscherm? Kan een social engineer het wachtwoord of dossiers ontfutselen? Wordt de werkplek vergrendeld als de werknemer zijn plaats verlaat?

[1] Het apparaat(device) is van oudsher de vaste computer maar steeds meer zijn dat mobiele apparaten.

3.3 Het apparaat

Wordt het apparaat zelf door de beheerder goed beschermd met virusscanners? Is de gebruiker verstandig met het aanklikken van linkjes en het installeren van onbekende software? Is het apparaat met wachtwoord beveiligd? Denk aan verlies van de mobiele telefoon die automatisch e-mail ophaalt.

Technische oplossingen voor veilige e-mail die in hoofdstuk 4 aan de orde komen, dekken deze kwetsbaarheid niet af. De veiligheid is afhankelijk van de hygiëne van de gebruikers en van beschermingsproducten als virusscanner, firewall en recente patches voor de software waarmee gewerkt wordt. Deze bescherming wordt hier verder buiten beschouwing gelaten. Veel maatregelen liggen in de opvoeding van de gebruikers in hun omgang met gevoelige informatie. Er ligt een taak bij security-officers en het management om hen bewust te maken van verantwoord gebruik van internet en hun apparatuur.

Kwetsbaarheden van devices
De bekende manieren om in te breken zijn gebaseerd op het vinden van het wachtwoord. De weg die in de eerste plaats open staat is: raden. Maar als men sterke wachtwoorden kiest is het installeren van malware op de computer van de gebruiker kansrijker. Malware is in staat om ingetikte wachtwoorden te onderscheppen. Ten derde is er de phishing techniek. Er komt een vertrouwenwekkend mailtje binnen met het verzoek om voor de zekerheid via een link nog eens aan te loggen. De link leidt je naar een nep website die je wachtwoord noteert. De bescherming van de werkplek tegen malware is daarom een eerste prioriteit. En de educatie van de gebruiker in het omgaan met binnenkomende verdachte e-mail is noodzakelijk.

Het is niet waarschijnlijk dat webmail gekraakt kan worden met zogenaamde brute force attacks, het automatisch in hoog tempo proberen van alle denkbare wachtwoorden. Providers hebben zich hiertegen beveiligd veelal door een serie van foute inlogpogingen te onderbreken met het vragen om een code uit een vaag plaatje in te tikken, CAPTCHA's. Iets waar menselijke interventie voor nodig is.

Een gat in de beveiliging is de procedure om een wachtwoord te resetten. De procedure is dat je controle vragen moet beantwoorden, zoals waar heb je je echtgenoot ontmoet. De Yahoo e-mail van Sarah Palin werd op die manier gekraakt, omdat een en ander op internet eenvoudig te achterhalen was. De dader heeft een jaar gevangenisstraf uitgezeten. Inmiddels hebben de meeste providers de procedures aangevuld met extra waarborgen.

3.4 De persoon zelf

Een ander veiligheidsaspect, als men de gehele keten beschouwt, is de persoon zelf: zijn de personen aan zenders- of ontvangerskant wel diegenen voor wie ze zich uitgeven? Een e-mail verzonden aan een e-mailadres kan volkomen veilig aankomen, maar wie zegt dat de persoon waarvan de verzender denkt dat hij achter dat e-mailadres zit, ook die persoon is?

Fragment 1. Afkomstig van forum security.nl

Deze kwetsbaarheid moet beschermd worden met maatregelen als in levende lijve[1] controle van iemands identiteit en vaststelling van het e-mailadres dat die persoon gebruikt. Op dit gebied bieden de meeste leveranciers geen soelaas. Vooral procedurele maatregelen zijn van toepassing om deze zwakke plek te beveiligen.

3.5 Het Verkeer van het apparaat naar de mailserver.

Het verkeer van apparaat naar server behoort altijd beveiligd te zijn[2]. Bij webmail is dat te zien door de HTTPS aanduiding voor de URL. Meeluisteraars op de lijn kunnen de communicatie dan niet ontcijferen. Sinds 15 maart 2014 met de ontdekking van het heartbleed-lek[3] in de openSSL software-library, die door veel webservers gebruikt wordt, moeten we de onkreukbaarheid hiervan nuanceren. Schokkend was dat een techniek die overal gebruikt werd, al jaren een lek kende. Ook al is dit lek gedicht, het roept wel de vraag op of er geen andere zwakheden bestaan.

3.6 E-mail opgeslagen bij een mailserver.

Is de informatie verblijvend op een mailserver veilig? Beheerders van de server kunnen e-mails vaak lezen. Zij zijn meestal gebonden aan geheimhoudingsverklaringen; ze zijn in dienst van een bedrijf en dus onderhevig aan een zekere controle. Het blijft echter zo dat ze het kùnnen inzien. Steeds meer providers kiezen ervoor het bericht versleuteld op de mailserver op te slaan, maar als de versleuteling plaatsvindt met een door de dienstverlener zelf gekozen sleutel dan wordt het lezen bemoeilijkt, maar niet onmogelijk.

3.7 Het transport van e-mails van server naar server.

De beveiliging van de lijn waarover een bericht van mailserver naar mailserver gaat, wordt steeds meer de praktijk[4]. Elke mailserver kan geconfigureerd worden zodat informatieverkeer over de lijn versleuteld verloopt. Daarvoor moet wel een certificaat op de mailserver geïnstalleerd worden. VPN en TLS zijn voorbeelden van technieken die dit verzorgen. Net zoals bij HTTPS kunnen luisteraars op de verbinding de informatie niet ontcijferen. Als mailservers in ziekenhuizen en instellingen nog niet zo beveiligd zijn, dan is een sterke aanbeveling om dat te controleren en configureren. Het is laaghangend fruit dat snel geplukt moet worden. Het NCSC heeft in november 2014 online een factsheet gepubliceerd over hoe je TLS moet implementeren.

4 De oplossingen

Het transport van informatie van apparaat naar server en van server naar server is steeds vaker versleuteld. De aanbieders van veilige e-mail die hier de revue zullen passeren hebben hun

[1] Ook wel bekend als face-to-face.
[2] Zie ook: https://www.google.com/transparencyreport/saferemail/
[3] https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-heartbleed-ernstige-kwetsbaarheid-in-openssl.html
[4] https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what#crypto-chart

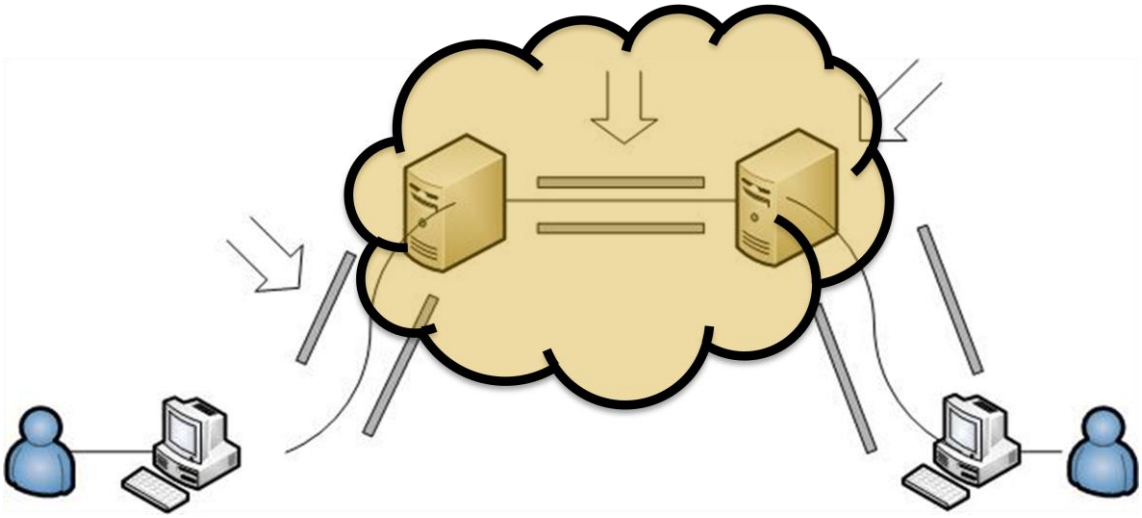
meerwaarde dus niet op dit vlak; zij bieden additionele beveiligingen, die we in twee categorieën indelen:

A. Veilige gecontroleerde lijnen en servers onder eigen beheer.
   De lijnen waarover wordt gecommuniceerd zijn in beheer bij één organisatie, of bij meerdere organisaties die elkaar vertrouwen. Niets verloopt over open internet. Het e-mailen gebeurt alleen met en via vertrouwde partners.
B. Bericht encryptie.
   Niet alleen het transport over de lijn is versleuteld maar ook alle berichten zijn zelf versleuteld. Als een bericht zelf is versleuteld dan is versleuteling van het transport eigenlijk overbodig. Vergelijk het met een ansichtkaart met een boodschap in geheimschrift; het maakt dan niet uit dat de postbode niet te vertrouwen is, hij kan het toch niet lezen.

Hieronder worden de oplossingen tegen het licht gehouden. 4.1 en 4.2, zijn voorbeelden van categorie A; 4.3 tot en met 4.6 zijn voorbeelden van B.

4.1 Één besloten e-mailomgeving

De berichtuitwisseling vindt plaats binnen één domein; de berichten blijven in één netwerk. Gebruikers kunnen onderling veilig e-mailen; ze benaderen de e-mail met een beveiligde verbinding. Toegang is mogelijk met gebruikersnaam en wachtwoord. Alle zorgvuldigheid met het kiezen en geheim houden van een wachtwoord is van toepassing.



Figuur 2. Eén besloten mailomgeving

ZorgMail van ENOVATION en Secure Mail van KPN bieden onder meer e-mail gebaseerd op dit model.

ZorgMail is van origine niet ontworpen om veilige e-mail te faciliteren. De eerste toepassingen waren het uitwisselen van gestructureerde informatie met EDIFACT berichten van systeem naar systeem. EDIFACT structureert de informatie in een bericht zodat een systeem ze kan ontleden en verwerken. Gaandeweg bleken ook zorgaanbieders zonder een eigen informatiesysteem behoefte te hebben aan die informatie. Voor hen zijn er e-mailboxes ingericht. De gestructureerde berichten werden omgezet in een voor een mens leesbaar formaat. Een volgende logische stap was dat de abonnees elkaar e-mail konden gaan sturen binnen de veilige infrastructuur. Zo is e-mail een toevoeging geworden op de dienstverlening.

Ook KPN heeft een EDIFACT dienstverlening. KPN heeft in samenwerking met een aantal zorgpartijen daarnaast een maildienst ontwikkeld om tegemoet te komen aan de steeds luidere

roep om betaalbare en gebruiksvriendelijke maildiensten.

Een besloten e-mailomgeving werkt vooral goed voor de abonnees. Correspondenten die geen account in dat domein hebben, zoals patiënten, kunnen niet veilig bereikt worden. Om daaraan tegemoet te komen hebben de aanbieders ZorgMail en KPN de mogelijkheid om veilig naar hen te mailen geopend.

Bij KPN krijgen patiënten[1] een notificatie in hun eigen e-mailbox als er een bericht klaarstaat in het veilige domein. Door op een link[2] te klikken en in te loggen komen zij in een beveiligde e-mailbox en kunnen de e-mail lezen. De eerste keer zullen zij een gebruikersnaam en wachtwoord moeten opgeven. Vanuit hun veilige e-mailbox binnen het veilige domein kunnen zij ook e-mails beantwoorden en initiëren, echter alleen aan ontvangers van wie zij eerder een bericht via KPN Secure Mail ontvangen hebben.

ZorgMail stuurt aan de patiënt [1] het gehele bericht versleuteld als PDF-bestand. Door een link te volgen - die ook in het bericht staat - kunnen ze het eenmalige wachtwoord ophalen uit een portaal, en het PDF bestand ontcijferen. Van daar uit kan de patiënt het bericht desgewenst beantwoorden.

Sterk punt van ZorgMail is het centrale adresboek. Abonnees kunnen in een telefoonboek andere adressen vinden. Omdat abonnees zich met waarborgen moeten aanmelden is er een zekerheid dat de zorgverlener die men een bericht wil sturen inderdaad beschikking heeft over dat e-mailaccount.

KPN en ENOVATION zijn belangrijke spelers in de zorgmarkt. Zij bieden naast de hierboven besproken oplossing gebaseerd op één besloten mail omgeving, ook de variant die hieronder in 4.2 wordt toegelicht.

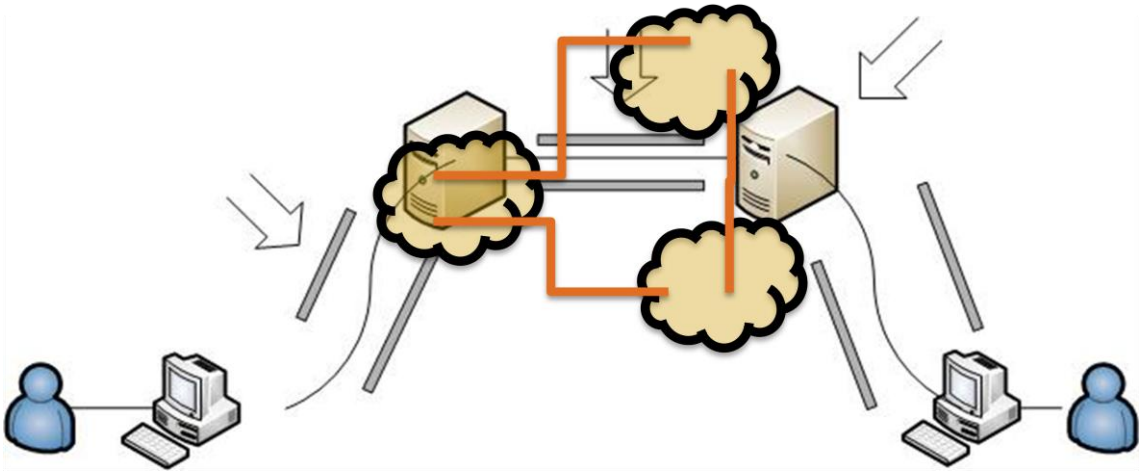
4.2 Gecombineerde vertrouwde mailomgevingen

Regionale netwerkorganisaties zoals stichting Zorgring Noord-Holland Noord, GERRIT en iZIT, hebben deze samenwerking vormgegeven. Ook ZorgMail en Secure Mail van KPN bieden deze vorm van veilige e-mail. Het principe is federatief. Regionale netwerken kennen elkaar en hebben met elkaar afgesproken dat ze e-mail van elkaar alleen zullen leiden over de verbindingen waar zij het beheer en de controle over hebben. Er wordt dus geen e-mail verstuurd over lijnen die niet bekend zijn. Dit wordt ook wel aangeduid als veilige relay of federatieve relay. De groep vertrouwde domeinen neemt toe. Steeds meer maildienstverleners sluiten zich aan via een veilige verbinding[3].

[1] Geldt voor alle niet op de besloten omgeving aangesloten ontvangers.

[2] Een keerzijde van het sturen van een link in een e-mail is dat op de manier ook phishing kan plaatsvinden.

[3] Veilig betekent hier òf een eigen lijn òf een gedeelde lijn waarover het verkeer versleuteld verloopt, en daarmee te betitelen is als een zo goed als eigen lijn. Vrije vertaling van virtual private network, VPN.



Figuur 3. Federatieve relay

Op elke mailserver binnen de samenwerking moet de lijst van vertrouwde domeinen aanwezig zijn, zodat de server kan beslissen of een geadresseerde via federatieve lijnen en dus veilig bereikbaar is. Patiënten zitten niet op de gecontroleerde infrastructuur en kunnen op deze manier dus niet veilig bereikt worden.

Ook ZorgMail Safe Relay van ENOVATION en Secure Mail van KPN zijn onderdeel van federaties[1]. Momenteel zijn alle partijen met elkaar in gesprek om samen te werken. Het zou heel mooi zijn als steeds meer aanbieders elkaars federaties zouden vertrouwen en verbinden, zodat ze een geheel vormen. De gebruikers kunnen dan in een klap veel meer mensen veilig bereiken. Belangrijk is wel dat de kwaliteit van de beheerorganisaties van de deelnemende partijen gewaarborgd is.

4.3 Berichtversleuteling/Encryptie van berichten

In categorie B bevinden zich de oplossingen waarbij de e-mail zelf versleuteld wordt; niet alleen over de lijn versleuteld verstuurd, maar ook onleesbaar op de mailserver staat. Het maakt niet uit hoe het bericht wordt getransporteerd. Alleen degene met de sleutel is in staat het bericht te lezen.

Versleuteling van berichten kent een lange geschiedenis, waar we nu niet op ingaan[2]. In de klassieke versleuteling spreken zender en ontvanger samen af welke geheime sleutel ze gaan gebruiken. De versleuteling die op het internet nu alomtegenwoordig is, is versleuteling gebruikmakend van een algemeen bekende openbare sleutel (Public Key Encryption). Iedere correspondent heeft een eigen sleutel, die iedereen mag kennen. Het fascinerende van deze methodiek is dat de versleuteling van een tekst verloopt met een openbare sleutel, maar dat de ontcijfering van de tekst niet kan plaatsvinden met dezelfde sleutel. Daarvoor is een tweede - geheime – sleutel nodig. Voor een vermoeden van hoe dit wiskundige hoogstandje in elkaar steekt zie onderstaand kader. Om kort te gaan heeft elke persoon een sleutelpaar, bestaande uit een publieke en een geheime sleutel. De publieke sleutel moet iedereen kennen die versleuteld naar hen wil e-mailen. De geheime moet geheim blijven.

[1] Zij hebben andere oplossingen om patiënten te bereiken, zoals beschreven in paragraaf 4.1.

[2] In de tweede wereldoorlog communiceerde men via radiogolven. Boodschappen gingen gewoon door de ether, door vriend en vijand op te pikken. De kunst was om de boodschap te kraken. Briljante wiskundigen in Cambridge o.l.v. van Alan Turing wisten de enigma versleuteling van de Nazi's te kraken. Volgens historici heeft die kraak de overwinning van de geallieerden enorm versneld.

Publieke sleutel encryptie

Dat een boodschap die vercijferd is met een sleutel, niet ontcijferd kan worden door iemand ook al heeft hij beschikking over dezelfde sleutel, is intuïtief moeilijk voor te stellen. Als je de sleutel hebt waar de fiets mee op slot is gezet, kun je hem toch ook weer openmaken? Nee, niet altijd.

De truc om met een publieke sleutel een tekst te coderen die met dezelfde sleutel niet ontcijferd kan worden, is gebaseerd op het ontbinden in factoren; iets wat ook mensen met een alfapakket zich kunnen herinneren van de middelbare school. Het getal 24 kan ontbonden worden in de factoren: (2 x 12); (3 x 8); (4 x 6);(3 x 2 x 4) etc. Als je twee grote priemgetallen p1 en p2 met elkaar vermenigvuldigt krijg je een getal dat maar op een manier te ontbinden is. Het blijkt heel moeilijk om van zo'n groot getal de twee factoren (p1 x p2) terug te vinden. Tot nog toe is de enige bekende methode het uitproberen van alle getallen. Als de priemgetallen groot genoeg zijn dan doet een supercomputer er jaren over om de oplossing te vinden. De vercijfering van een tekst met de publieke sleutel is wiskundig zo ontworpen dat de ontcijfering alleen mogelijk is als je de ontbindende factoren kent. Alleen degene die p1 en p2 kent, kan het bericht ontcijferen.

Terug naar de fiets. Stel je voor dat je vele hangsloten hebt en één sleutel waarmee je die sloten open kan maken. En je legt je hangsloten opengeklikt op een voor iedereen toegankelijke plek. Dan kan iedereen een slot van jou pakken en iets – een fiets, een kistje - met het slot dichtklikken. Niemand behalve jij kan het daarna openmaken. Zo werkt het ook in de cryptografie. De publieke sleutel is het open hangslot dat overal beschikbaar is. Iedereen kan het gebruiken en iets op slot zetten. Alleen jij kan met je privé sleutel het hangslot openen. Op youtube zijn een aantal aardige filmpjes die dit illustreren: http://www.youtube.com/watch?v=U62S8SchxX4 ; http://www.youtube.com/watch?v=56fa8Jz-FQQ, zie ook *Figuur 4*.

Het versleutelen van berichten met deze techniek heeft niet de hoge vlucht genomen die men verwachtte bij de eerste introductie. In de praktijk blijkt het een uitdaging om iedereen te voorzien van sleutels. Als je iemand wilt e-mailen moet je diens publieke sleutel ergens vinden. Je moet weten of die sleutel nog geldig is. De geadresseerde moet al een publieke sleutel hebben. Je kunt dus niet onvoorbereide ontvangers een versleutelde e-mail sturen.

Figuur 4. Verzender beschikt over de publieke sleutels(sloten) van haar vaste contactpersonen

PKI

Het beheren van sleutels is de grootste uitdaging gebleken. Om dat goed te kunnen doen zijn algemeen toegankelijke voorzieningen nodig. Die voorzieningen voor publicatie, verificatie en intrekking van sleutels zijn dusdanig omvangrijk dat ze de naam infrastructuur verdienen, vandaar de term PKI, Public Key Infrastructure. Aanmaak van sleutelparen moet onder controle staan van dienstverleners die volledig betrouwbaar zijn en staan onder een stringent regime van beveiliging. Het inrichten en onderhouden van die infrastructuur maakt dat het grote succes van PKI voor encryptie van e-mail nog uitblijft. PKI is wel succesvol in sleutels voor systemen(Certificaten). Alle hiervoor geschetste transport beveiligingstechnieken (SSL, VPN, TLS) zijn gebaseerd op PKI. De distributie van certificaten naar personen is tot nog toe te minder van de grond gekomen. Een uitzondering is overigens de UZI-pas.

4.4 PGP en verwanten

Een implementatie in het publieke domein van publieke sleutel encryptie is PGP, Pretty Good Privacy. De 'infrastructuur' om sleutels te beheren wordt verzorgd door de gebruikers zelf. De gebruiker gebruikt een PGP key generator om zijn publieke en geheime sleutel te berekenen. Hij bewaart zijn geheime sleutel. De gebruiker zal moeten zorgen dat zijn publieke sleutel bekend is. PGP gebruikers vermelden die vaak onderaan een e-mail.

Er zijn websites waar ze aangemeld kunnen worden. Andere gebruikers die jou kennen, kunnen bevestigen dat jouw sleutel betrouwbaar is. In de praktijk vereist deze manier van versleutelen kennis van zaken. PGP is een tool dat vooral door liefhebbers gebruikt wordt. Bij de NCSC en faculteiten informatica is het populair. Dat komt vast omdat het gebruiken van PGP kennis vereist, maar misschien ook omdat deze categorie beter doordrongen is van de risico's van berichtonderschepping en privacy hoog in het vaandel heeft staan.

4.5 Identity Based Encryption

Een nieuwe aanbieder op de markt is Voltage Security, met hun implementatie van Identity Based Encryption (IBE). Zij maken gebruik van publieke sleutel encryptie maar met een slimmigheidje. De 'publieke' sleutel die gebruikt wordt om een bericht te versleutelen wordt gegenereerd met als parameters onder meer het e-mailadres van de ontvanger. Dit gebeurt door een centrale voorziening (server). De verzender biedt het adres van de ontvanger aan en krijgt van de server een openbare sleutel. De verzender versleutelt zijn post met die sleutel en verstuurt het. De ontvanger kan het bericht ontcijferen door bij de centrale voorziening zijn geheime sleutel op te halen. Deze afhandeling gebeurt achter de schermen. De verzender moet in zijn e-mailprogramma - veelal outlook – niet op de send-knop maar op de send-secure knop drukken. De ontvanger zal de e-mail

meteen ontcijferd in zijn inbox aantreffen. In bovenstaande situatie zijn de correspondenten beide abonnee van Voltage.

Het is ook mogelijk om een niet-abonnee een secure e-mail te sturen. Hetzelfde mechanisme is van kracht. De ontvangers moeten alleen iets meer doen om het bericht te ontcijferen. Ze krijgen een versleutelde e-mail in hun eigen e-mailbox en via een link kunnen ze het bericht aanbieden aan de Voltage Keyserver, die het zal ontcijferen en tonen. De eerste keer zullen zij gebruikersnaam en wachtwoord moeten aanmaken om een account op de key server te krijgen. Dit is functioneel gelijk aan de ZorgMail oplossing waarbij een versleutelde PDF aan de patiënt verstuurd wordt.

IBE is een open standaard. Voltage heeft er eigen vindingen aan toegevoegd die het tot een uitrolbaar product maken.

Voor abonnees is ook digitale ondertekening van berichten beschikbaar. Dat waarborgt niet alleen de vertrouwelijkheid van berichten maar ook de integriteit en authenticiteit.

4.6 Veilige e-mail met de UZI-pas

De UZI-pas is goed te gebruiken in de zorg voor een zeer veilige e-mailuitwisseling. Het heeft ook de mogelijkheid een digitale handtekening te zetten. De persoon in bezit van de pas heeft in levende lijve zijn pas opgehaald. Zijn identiteit is vastgesteld. Een complete infrastructuur bestaat om publieke sleutels te vinden. Op www.uziregister.nl[1] is te vinden hoe de UZI-pas gebruikt kan worden voor digitale ondertekening van e-mail. Ook versleuteling van het bericht en de bijlagen is mogelijk. Wel moet men kennis van zaken hebben om het in gebruik te nemen. Het is echter goed mogelijk om software te bouwen of handleidingen te schrijven waarmee de toepassing van encryptie met de UZI-pas veel gemakkelijker wordt. Tot nog toe is dat idee wel eens geopperd, maar nog nooit echt van de grond gekomen.

Oplossing voor kleine zelfstandigen in de zorg.
Een psychotherapeut die haar cliënten zou willen e-mailen kan voor een pragmatische oplossing kiezen. Zij zou tijdens een consult met de cliënt kunnen afspreken welk wachtwoord zij samen gaan gebruiken als sleutel om documenten met gevoelige gegevens te versleutelen. Het mooie is dat ze in levenden lijve vaststelt wie de cliënt is en welk e-mailadres hij gebruikt. De cliënt kan meteen zijn toestemming geven voor het versturen van zijn gegevens. Als beiden een wachtwoord overeenkomen dan kan de therapeut ’s avonds het dossier versleuteld verzenden. Zelfs de hotmails en gmails kunnen gebruikt worden omdat de bijlagen niet gelezen kunnen worden zonder wachtwoord. Microsoft Word en Acrobat bijvoorbeeld, hebben de mogelijkheid om een document met een sterke encryptie te versleutelen. Het feit dàt er contact is met een psychotherapeut blijft natuurlijk niet verhuld. Zie ook bron: (LVMP)

5 Conclusies

In dit hoofdstuk laten we de verschillende soort oplossingen nogmaals de revue passeren. Ditmaal gaan we op verschillende aspecten na hoe ze zich tot elkaar verhouden. De vier die we vergelijken zijn:

1. Één besloten mailomgeving
2. Federatie van vertrouwde infrastructuren

[1] http://www.uziregister.nl/uzipas/nieuweklant/watkanikmeteenuzipas/elektronischehandtekening/

3. Identity Based Encryption
4. PGP/UZI pas

5.1 Gebruikersvriendelijkheid

Bij het gebruik van de federatieve relay merkt de gebruiker niets van de aanpassing. Automatisch worden e-mails - als het kan - over de gecontroleerde lijnen verstuurd. Als men kiest voor één besloten e-mailomgeving, zoals ZorgMail en KPN die onder meer bieden, krijgt men een ander (tweede) e-mailadres. Met de gangbare e-mailprogramma's is het mogelijk dat account naast het eigen account open te hebben en dus gemakkelijk beide e-mailboxes te monitoren. Als men een e-mail veilig wil versturen moet men de e-mail verzenden vanuit de veilige e-mailbox.
Bij Voltage behoudt men het eigen e-mailaccount. Maar in - bijvoorbeeld - outlook, verschijnt er een tweede verzendknop met het label Send-secure.
Veilige e-mail met PGP en UZI-pas zijn qua ingebruikneming als minder gebruikersvriendelijk getypeerd. Na installatie zal het dagelijks gebruik wel eenvoudiger zijn, maar niet in de buurt komen van de andere drie.

5.2 Functionaliteit zorgverlener -> patiënt

Federatieve relay beveiligt niet de communicatie van zorgverlener naar patiënt. De PGP-oplossing kan dat alleen als de patiënt PGP gebruikt. De UZI-pas staat niet ter beschikking van de patiënt. KPN, ZorgMail en Voltage kunnen het wel. De functionaliteit is vanuit gebruikersoogpunt gelijk. Bij alle drie ontvangt de patiënt een mail in de eigen mailbox. Bij KPN bevat de e-mail een link. Via die link komt men op de veilige infrastructuur en kan men daar het bericht lezen. Voltage en ZorgMail leveren het gehele bericht als een versleutelde bijlage af bij de gebruiker. Dat biedt een voordeel omdat de berichten niet aanwezig zijn op de server. Men opent de bijlage en de ontcijfering wordt in gang gezet door de sleutels op te halen bij de server. Bij alle drie moet men de eerste keer een wachtwoord aanmaken.

5.3 Authenticatie

Onder authenticatie verstaan we het zeker stellen dat het e-mailadres behoort bij de persoon die je wenst te bereiken[1]? Bij de federatieve relay wordt er veilig ge-e-maild tussen werknemers van bedrijven die behoren tot een vertrouwd domein. Aangezien de werknemers bij hun aanstelling hun paspoort hebben overlegd, is het behoorlijk zeker dat achter het e-mailadres ligtvoet@nictiz.nl, Maarten Ligtvoet, werknemer van Nictiz, te bereiken is.

Dit geldt ook voor de abonnees van ZorgMail, KPN en Voltage. Dit geldt echter niet voor de niet abonnees – lees patiënten. De zekerheid dat achter valiente34@xs4all.nl de heer Jansen schuilt, moet op een andere manier verkregen worden. Bijvoorbeeld, op consult kan men de patiënt vragen naar zijn e-mailadres en dat nauwkeurig noteren.

De zekerheid over iemands identiteit is in bovenstaande gevallen gebaseerd op procedures, zoals bij indiensttreding. Voltage biedt net als PGP en UZI-pas, aan abonnees de mogelijkheid om een bericht digitaal te ondertekenen; de authenticatie is gebaseerd op cryptografie. Het is zeker dat alleen de eigenaar van de geheime sleutel de e-mail kan hebben ondertekend. De infrastructuur moet waarborgen dat de geheime sleutel alleen in het bezit kan zijn van de gerechtigde persoon.

5.4 End-to-end encryption

PGP en UZI-pas en IBE[2] bieden end-to-end encryption. Het bericht is vanaf vertrek tot en met eindstation versleuteld. Implementaties van Voltage in instellingen bestaan meestal uit het inrichten van een e-mail-verzamelpunt, een gateway, waar het bericht ontcijferd wordt. Dat

[1] conform de STORK classificatie bestaan er overigens vier betrouwbaarheidsniveaus van authenticatie zie o.a. Handreiking Patiëntauthenticatie (Nictiz, 2013). Voor iedere toepassing kan het gewenste niveau verschillen.
[2] IBE kent wel een derde entiteit, de key-server, die theoretisch in staat is de e-mail te ontcijferen.

betekent in dat geval dat transport van het bericht van gateway naar eindgebruiker niet versleuteld is. Dit wordt als veilig gezien omdat het verkeer binnen de instelling betreft. Overigens kan Voltage ook zonder gateway werken zodat berichten pas op het apparaat binnen de instelling van de eindgebruiker ontcijferd wordt.

Aspecten	Één domein	Federatie	IBE	PGP/UZI pas
Gebruikersvriendelijk	●	●	●	○
Niet merkbaar voor gebruiker	○	●	○	○
Patiënten veilig te bereiken	●	○	●	○
Authenticatie deelnemers	●	●	●	●
Authenticatie buitenstaanders	○	n.v.t.	○	n.v.t.
Digitale handtekening	○	○	●	●
Integratie met eigen account	○	●	●	●
End-to-end encryption	○	○	●	●

Tabel 1. Samenvattende beoordeling van de mailoplossingen op verschillende aspecten. De open bullet betekent dat een mailoplossing niet voldoet aan een aspect. Een gesloten bullet geeft aan dat de oplossing voldoet.

5.5 Vendor lock-in

Er is bij geen van de oplossingen werkelijk sprake van Vendor-lock in[1]. Je kunt er zonder meer van af. Let wel, elke verandering van e-mailadres en e-mailbox is natuurlijk bewerkelijk. Mensen die wisselen van e-mailadres, moeten iedereen op de hoogte brengen en alle berichten die in die e-mailbox zitten veiligstellen. Hetzelfde geldt voor de berichtenboxen van ZorgMail en Secure Mail van KPN. Voltage garandeert dat e-mails voor niet-abonnees altijd ontcijferbaar blijven via de voltage-server. Mocht Voltage geheel verdwijnen, dan moeten e-mails via knippen en plakken in een ander formaat worden opgeslagen.

5.6 Interoperabiliteit

Ofschoon het e-mail-landschap versnipperd is, betekent het niet dat de verschillende oplossingen niet met elkaar werken. Vanuit het oogpunt van een patiënt is echter het volgende mogelijk. Als hij naar drie zorginstellingen gaat waarvan er één ZorgMail van ENOVATION, de tweede Secure Mail van KPN en de derde Voltage heeft. En hij krijgt van alle drie elektronische post, dan zal hij drie verschillende plaatsen op internet moeten bezoeken om zijn post te lezen.

Zoals eerder al gesteld, zou het mooi zijn als alle aanbieders van veilige relay-oplossingen: ZorgMail, KPN en de regio's elkaar als vertrouwde partijen zouden accepteren en zo de schaal van vertrouwde domeinen enorm vergroten. Als het aantal deelnemers toeneemt is het handig om de betrouwbaarheid van de deelnemers te laten toetsen door een onafhankelijke autoriteit. Het keurmerk Zorg Service Provider(ZSP) zou als een voorwaarde voor toetreding tot de federatie kunnen gelden.

6 De toekomst

De noodzaak om ad hoc ongestructureerde informatie uit te wisselen zal altijd bestaan. Voorlopig

[1] Vendor lock-in maakt een klant afhankelijk van een leverancier voor producten en diensten, omdat hij niet in staat is om van leverancier te veranderen zonder substantiële omschakelingskosten.

zal e-mail daarvoor een belangrijk middel zijn. Als een situatie die vraagt om informatie-uitwisseling regelmatig optreedt en als de informatie steeds van de zelfde aard is, dan ligt het voor de hand om de uitwisseling te structureren en niet meer via e-mail plaats te laten vinden. Denk aan de aanvraag voor een herhaalrecept. Dan is het beter om een webpagina te ontwerpen die de patiënt kan invullen[1]. Het invullen van een webpagina op een server kent minder kwetsbaarheden dan e-mail omdat de weg die informatie aflegt korter is. Een veilig e-mailproduct is dan niet nodig. Een ander voordeel is dat de gestructureerde informatie gemakkelijker te verwerken is in systemen.

De elektronische communicatie met de patiënt zal steeds meer geïntegreerd worden in de informatiesystemen van zorgaanbieders. Een aanvraag voor een herhaalrecept zou typisch direct in het informatiesysteem terecht moeten komen. Ook uitgaande e-mail zou direct vanuit een huisartsinformatiesysteem (HIS) plaats moeten vinden. Het kan niet anders of leveranciers van informatiesystemen en die van veilige e-mailoplossingen zullen elkaar daarin gaan versterken.

Voorlopig is het veilige e-mail-landschap in de zorg versnipperd. Dat hoeft niet erg te zijn. Het is de vraag of één oplossing voor alles het juiste recept is. De overheid zou zich als verkeersregelaar kunnen opwerpen door de standaarden te ontwerpen, of zelfs als provider van een veilige infrastructuur. Met de geschiedenis van het landelijk EPD in het achterhoofd, is de politieke haalbaarheid van het laatste twijfelachtig. Iets vergelijkbaars bestaat wel, via de website mijnoverheid.nl, waarop je als burger een account kunt maken en berichten van belastingdienst, RDW en anderen ontvangen.

De kans om met de UZI-pas de communicatie van zorgverlener naar zorgverlener volledig te beveiligen bestaat nog steeds. Het is niet per se noodzakelijk dat die communicatie over een centrale landelijke infrastructuur verloopt. Wel is nodig dat er tools ontwikkeld worden die het gebruik vergemakkelijken. Deze weg komt in de toekomst misschien zelfs beschikbaar voor alle burgers. eID is een project van het ministerie van Binnenlandse Zaken (BZK) dat elektronische authenticatie voor iedereen regelt; de opvolger van DigiD.

Als eID succesvol wordt zal dat leiden tot beschikbaarheid van authenticatiemiddelen en encryptie voor bedrijven én burgers. Dan kan veilige uitwisseling op die leest geschoeid worden. Een succesvol eID programma kan baanbrekend worden in de mogelijkheden voor burgers om zich in het maatschappelijk verkeer te authenticeren en versleuteling toe te passen in de communicatie. Het biedt de mogelijkheden die DigiD nu biedt. Maar aangezien het veel veiliger is (in ontwerp) zal de toepassing veel breder worden. Of eID naast authenticatie ook encryptie zal faciliteren is overigens nog niet bepaald.

Tot slot
Wij hopen dat deze verkenning een handreiking is voor een afweging van maatregelen ter beveiliging van e-mail. Er is laaghangend fruit: zorg voor certificaten op de eigen mailservers en dwing e-mailtransport met beveiligde verbinding af. Overweeg, als kleine praktijkhoudende zorgverlener, een e-mailprovider te contracteren die belooft de vertrouwelijkheid van communicatie te respecteren.

Wilt u van gedachten wisselen over veilige e-mail in de zorg of meer informatie? Neem dan contact op met Jan Jongenelen of Maarten Ligtvoet, respectievelijk via jongenelen@nictiz.nl of ligtvoet@nictiz.nl.

7 Over de auteurs

[1] De webpagina moet dan wel veilig zijn. Zie hiervoor “beveiligingsrichtlijnen voor webapplicaties” van het NCSC.

Jan Jongenelen studeerde medische informatica aan de Universiteit van Amsterdam. In 2009 kwam hij in dienst bij Nictiz als productmanager van het Landelijk Schakel Punt (LSP). Na het verwerpen van de wet op het EPD heeft hij zich gericht op kwalificaties van informatiesystemen. Zijn werkervaring ligt op het gebied van overheid en ICT. Met als focus Informatiebeveiliging.

Maarten Ligtvoet studeerde bio-informatica aan de Universiteit Leiden. Sinds een paar jaar heeft hij zijn passie voor open source software kunnen vormgeven in zijn huidige rol als productmanager ART-DECOR: een platform om (open) zorginformatiestandaarden op te ontwikkelen en beheren. Verder werkt hij aan informatiebeveiliging en kwalificaties van zorginformatiesystemen.

8 Geraadpleegde bronnen

- Boneh, F. (sd). *Identity-Based Encryption from the Weil Pairing.* Opgehaald van http://crypto.stanford.edu/~dabo/abstracts/bfibe.html
- CBP. (2013). *CBP Richtsnoeren beveiliging persoonsgegevens.*
- LVMP. (sd). *http://www.lvmp.nl/beheer/wp-content/uploads/Vuistregels.beveiliging.digitaleclt.dossiers1.pdf.* Opgehaald van www.lvmp.nl.
- Menno Schoonhoven, J. K. (2009). *onderzoek secure email voor de gezondheidszorg.* Atos Consulting.
- NCSC. (2014). *Cybersecuritybeeld Nederland.* Den Haag: NCSC.
- Nictiz. (2013). *Handreiking Patiëntauthenticatie.*
- Olsthoorn, P. (2014, januari 1). Spionage in Nederland: de onderbuik en de feiten. *HP De Tijd* .
- Reijnoudt, M. (sd). *https://decorrespondent.nl/997/Gevoelige-medische-dossiers-worden-vaak-illegaal-onbeveiligd-rondgemaild/92872778295-9d14cd2b.*
- Schneier, B. (sd). *https://www.schneier.com/*.
- *The Identity-Based Encryption Advantage.* (sd). Opgehaald van http://www.voltage.com/wp-content/uploads/Voltage_Technical_Brief_SecureMail_The_IBE_Advantage.pdf
- UZI-register. (sd). *Elektronische ondertekening van e-mail met Microsoft Outlook.* Opgehaald van http://www.uziregister.nl/doc/pdf/Ondertekenen%20e-mail%20met%20Microsoft%20Outlook%20(UZ69.03)_37585.pdf
- *ZorgMail voorwaarden.* (sd). Opgehaald van http://www.zorgmail.nl/attachments/article/101/Voorwaarden%20ZorgMail%20Eerstelijn szorgverleners.pdf.
- ZorgMail. (sd). *ZorgMail Secure e-mail.* Opgehaald van http://www.zorgmail.nl/attachments/article/101/ZorgMail%20Secure%20e-mail.pdf.

9 Lijst met afkortingen

IBE	Identity Based Encryption
CA	Certificate Authority
CBP	College bescherming persoonsgegevens
NCSC	Nationaal Cyber Security Centrum
eID	electronische identiteit
PKI	Public Key Infrastructure
SSL	Secure Socket Layer

VPN	Virtual Private Network
TLS	Transport Layer Security
RDW	Rijksdienst voor het Wegverkeer
LSP	Landelijk Schakelpunt beter bekend als landelijk EPD
PGP	Pretty Good Privacy
UZI	Unieke Zorgverlener Identificatie
WBP	Wet Bescherming Persoonsgegevens

Optimale toepassing van eHealth en ICT in de zorg kan niet zonder standaardisatie. In nauwe samenwerking met zorgverleners, koepelorganisaties, standaardisatieorganisaties en industrie draagt Nictiz zorg voor de ontwikkeling en beschikbaarheid van de noodzakelijke standaarden. We doen dit door het organiseren van gemeenschappelijke ontwikkelprojecten, kennisoverdracht en kwaliteitstoetsing.

Nictiz
Postbus 19121
2500 CC Den Haag
Oude Middenweg 55
2491 AC Den Haag

T 070 - 317 34 50
@Nictiz
info@nictiz.nl
www.nictiz.nl