Veilig mailen in de zorg

Verkenning van maildiensten bij het voorkomen van datalekken

rzcc

Regionaal ZorgCommunicatie Centrum • Juli 2016

Management **samenvatting**

U heeft er ongetwijfeld al eens van gehoord: **datalekken.** Een zoekgeraakte USB-stick met persoonsgegevens, een gehackte laptop of een e-mail die via een verkeerde mailinglijst wordt verzonden; een datalek doet zich regelmatig voor. Het verloren gaan of onrechtmatig gebruiken van persoonsgegevens is dan ook een hot issue in het maatschappelijk debat.

Sinds 1 januari 2016 verplicht de Wet bescherming persoonsgegevens (Wbp) zorgorganisaties om datalekken waar mogelijk te voorkomen en passende maatregelen te nemen wanneer het zich toch voordoet. Het mogelijke gevolg van een datalek is daarmee niet alleen imagoschade, maar ook de boetes kunnen enorm oplopen. Een deel van de beveiligingsincidenten in de gezondheidssector wordt veroorzaakt door menselijke fouten, waaronder verkeerde adressering of het onveilig beschikbaar stellen van persoonlijk of medische data (Verizon, 2015). Dit vormt een behoorlijke uitdaging voor zorgorganisaties, zeker gezien het feit dat een belangrijk deel van communicatie van zorgorganisaties via e-mail verloopt!

Gelukkig zijn er verschillende veilige maildiensten die ondersteunen in het verminderen van datalekken. Het Regionaal Zorg Communicatie Centrum (RZCC) te Eindhoven heeft deze vergelijking opgesteld, zodat aangeboden diensten inzichtelijk zijn en zorgorganisaties een goede keuze kunnen maken voor een veilige maildienst. Centraal hierbij stellen we de vraag in welke mate deze diensten actief ondersteunen bij de reductie van de kans op datalekken. Vanwege de risico's die optreden bij het gebruik van e-mail, worden in deze vergelijking zowel eisen gesteld aan de gebruiker als aan de techniek/infrastructuur. Het RZCC vergelijkt de diensten KPN Secure Mail ('KPN E-zorg'), HPE SecureMail ('Voltage'), Sophos SPX en ZIVVER en weegt de voor- en nadelen van deze diensten tegen elkaar af. De leveranciers van de veilige maildiensten hebben de vergelijking ingezien en hun reviews zijn meegenomen in het rapport.

We beschrijven dat het risico op datalekken zich in drie stadia van het verzendproces kan voordoen: vóór het verzenden, tijdens het transport en na het ontvangen. Uit de vergelijking blijkt dat de diensten sterk variëren in hun visie op veilige mail en in de rol die het systeem speelt bij het voorkomen van datalekken.

Naast de mate waarin diensten voor veilige mail bijdragen aan het verminderen van het risico op datalekken, vergelijken we de diensten ook op implementeerbaarheid & gebruiksgemak en op kosten & besparingen voor zorginstellingen. Wat betreft implementeerbaarheid blijkt dit voor alle diensten verhoudingsgewijs redelijk eenvoudig in uitvoering te brengen zijn.

Op het gebied van gebruiksgemak, is er meer verschil tussen de diensten. We hebben het gebruikersgemak vergeleken voor de verzender, de ontvanger die de dienst ook gebruikt en de ontvanger die zelf geen gebruiker is van de dienst. Er zijn diensten die naast het zorgen voor 'technische beveiliging' zich specifiek richten op het bewust maken van de gebruiker van zijn mailgedrag en hierdoor datalekken proberen te voorkomen. En er zijn diensten die meer op de achtergrond werken om datalekken te voorkomen. Beide werkwijzen hebben gevolgen voor het gebruiksgemak: een dienst die meer op de achtergrond werkt is minder aanwezig en zichtbaar dan een dienst welke actief de gebruiker op zijn mailgedrag attendeert.

Het RZCC is van mening dat bewustwording bij de gebruiker m.b.t. het gepast omgaan met patiëntinformatie en andere privacygevoelige gegevens een groot goed is. Deze bewustwording is een wisselwerking tussen systeem en eindgebruiker. Elke zorgorganisatie dient voor zichzelf te bepalen in hoeverre zij haar medewerkers dient te faciliteren in het veilig mailen en welke rol een veilige mail oplossing hierin kan spelen.

De kostenvergelijking is op basis van een fictieve zorgorganisatie gedaan. De standaardkosten van de diensten verschillen nogal van elkaar waarbij regionale afname kan leiden tot reductie. De mate van besparing hangt samen met de geboden beveiliging en gebruiksvriendelijkheid. Deze besparingen omvatten naast tijdswinst en vervanging van communicatiemiddelen ook vermindering van risico op imagoschade en boetes.

Concluderend hebben de leveranciers verschillende visies op mailen en de rol die het systeem en eindgebruiker hierin beiden (moeten) spelen. Één meest geschikte oplossing voor elke organisaties of regio is niet te geven. Dit is afhankelijk is van de wensen, eigenschappen en risicolandschap van een organisatie of de prioriteit die een regio aanbrengt. Deze analyse laat zien dat een gezamenlijke regionale keuze voor een veilige maildienst voordelen biedt. Regionaal gebruik leidt tot meer gebruiksgemak, lagere kosten en door eenduidig gebruik tot meer veiligheid.

Last but not least is het een feit dat ondanks alle mogelijke IT-oplossingen datalekken niet waterdicht opgelost kunnen worden. Zolang de menselijke component deel blijft uitmaken van het proces zal er een risico op datalekken blijven. Hoe groter het uitsluiten van menselijke handelingen, hoe kleiner het risico op datalekken.

Met de wetenschap dat de individuele afweging / best passende oplossing per afzonderlijke organisatie kan verschillen, lijkt ZIVVER momenteel een geschikte keuze voor een veilige email-dienst. Deze dienst geeft, in deze analyse, de meest complete bescherming tegen datalekken op basis van de diverse casussen en is voor uiteenlopende doelgroepen (zorgverleners onderling, externen en de cliënt/patiënt) het meest gebruiksvriendelijk.

Note van de redactie: VANAD Enovation is van mening dat dit onderzoek niet op basis van juiste gegevens heeft plaatsgevonden en heeft derhalve besloten niet in deze rapportage opgenomen te willen worden. Voor meer informatie over de diensten van VANAD Enovation, kunt u zich wenden tot hen.

Inhoud

1. Waarom dit document? 6

1.1 Aanleiding 6
1.2 Opgave 6
1.3 Beperkingen van dit onderzoek 6
1.4 Leeswijzer 6

2. Achtergrond en onderzoeksopzet 7

2.1 Datalekken in de gezondheidszorg 7
2.2 Aanpak 7
2.3 Conclusie 8

3. Opzet en werking van diensten voor veilige mail 9

3.1 KPN Secure Mail Premium (E-Zorg) 9
3.2 HPE SecureMail (Voltage) 10
3.3 Sophos SPX: SPX e-mail encryption 10
3.4 ZIVVER 10

4. Reductie van risico op datalekken 12

4.1 Signalering gevoelige content 12
4.2 Signalering adresseerfouten 14
4.3 Bescherming tegen hacken tijdens verzending 17
4.4 Verzekering dat alleen de ontvanger toegang heeft tot het bericht 18
4.5 Bescherming na verzenden 19
4.6 Bijdrage aan bewustwording omtrent datalekken in organisatie 20
4.7 Beschikbaarheid van logging-informatie (t.b.v. rapportage en monitoring) 21
4.8 Totaaloverzicht functionaliteiten t.b.v. voorkomen datalekken 22

5. Implementatie en gebruiksgemak 23

5.1 Wijze van implementatie 23
5.2 Gebruiksgemak 23

6. Kosten en besparingen veilige maildiensten 25

6.1 Kosten van de diensten 25
6.2 Besparingen 25

7. Conclusie 26

1. Waarom dit document?

1.1 Aanleiding

In welke mate zorgverleners gebruik maken van onbeveiligde e-mail is niet precies te bepalen. Dát het gebeurt, is een feit. Waar tot voor kort alleen *security officers* zich ongerust maakten over de risico's van het uitwisselen van privacygevoelige gegevens, hebben de media tegenwoordig ook steeds vaker aandacht voor dit thema en is het onderwerp van maatschappelijk debat. De wetgeving met betrekking tot de bescherming van persoonsgegevens (Wbp) verplicht zorgorganisaties per 1 januari 2016 om alles binnen het redelijke te doen om *datalekken* te voorkomen en passende maatregelen te nemen wanneer het toch voor komt. Zo stelt de Wbp onder andere dat de instelling als verantwoordelijke melding doet na ontdekking van een beveiligingsincident die nadelige gevolgen heeft/zal hebben voor de bescherming van persoonsgegevens van één of meerdere betrokkenen. Daarnaast bepaalt de wet dat de instelling zo snel mogelijk redelijke maatregelen moet nemen, om nadelige gevolgen van een datalek te herstellen of zoveel mogelijk te beperken.

1.2 Opgave

Het RZCC ondersteunt zorgorganisaties bij het realiseren van veilige communicatie voor medewerkers en cliënten. Daarom hebben we verschillende diensten van leveranciers in veilige mailoplossingen verkend. Centraal hierbij stellen we de vraag **in welke mate deze diensten ondersteuning bieden om de kans op datalekken te verkleinen**. We focussen daarbij op veilige maildiensten die zowel communicatie in de keten als met externen en de cliënt/patiënt mogelijk maken. Ook richten we ons enkel op de emailfunctie van deze leveranciers. De gekoppelde/aanvullende diensten zoals Edifact koppeling, overdracht van grote bestanden, virusscanning en veilig chatten nemen we dus niet mee in deze vergelijking.

1.3 Beperkingen van dit onderzoek

We baseren deze notitie op de door leveranciers beschikbaar gestelde informatie via internet (desk research) en op productinformatie die additioneel is opgevraagd bij de leveranciers. Het functioneren van de diensten in de daadwerkelijke praktijkomgeving is niet meegenomen. Door deze werkwijze kan het zo zijn dat de weergave in dit document afwijkt van de werkelijke situatie. Ook kunnen de diensten zich op onderdelen hebben ontwikkeld of aangepast. Dit document is daarom enkel bedoeld om in grote lijnen inzicht te krijgen in de werking van verschillende diensten **op dit moment.** Dit geldt eveneens voor de investeringen/kosten van de diensten, die bepaald zijn op basis van universele en standaard tarieven van de leveranciers. *De leveranciers van de veilige maildiensten hebben hun deel van de vergelijking vooraf ingezien en hun reviews zijn meegenomen in het rapport.* Omdat de actuele en situationele informatie over de werking, compatibiliteit en de kosten van diensten kan variëren en kan afwijken, wordt aanbevolen om voor nadere informatie contact op te nemen met de leveranciers.

1.4 Leeswijzer

In hoofdstuk 2 gaan we eerst in op de achtergrond en de opzet van het document. In hoofdstuk 3 geven we vervolgens globaal de visies en werking van de verschillende veilige maildiensten weer. Hoofdstuk 4 beschrijft de functionaliteit van de diensten op basis van een aantal onderscheiden stappen in het verzendproces. Vervolgens geven we een overzicht van implementatie- en gebruiksgemak in hoofdstuk 5. In hoofdstuk 6 gaan we in op de kosten en de mogelijke besparingen per oplossing. We sluiten af met een conclusie van de bevindingen.

2. Achtergrond en onderzoeksopzet

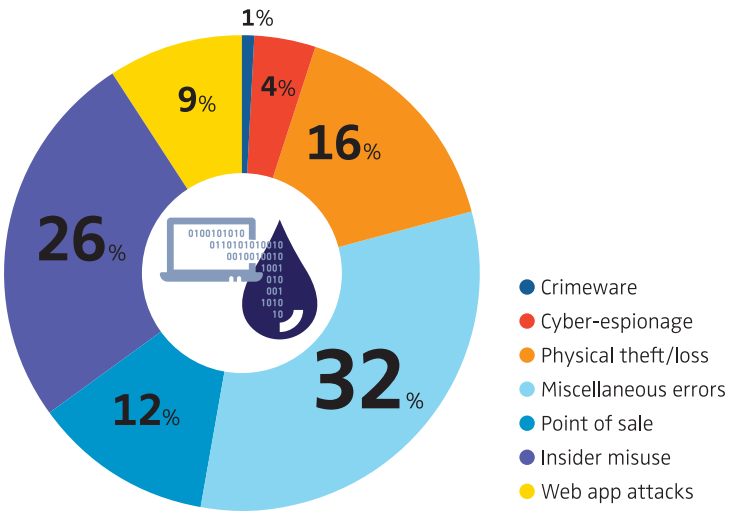
2.1 Datalekken in de gezondheidszorg

Volgens de wet is er sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren gaan, of als onrechtmatig gebruik van persoonsgegevens niet is uit te sluiten.

Als zich een beveiligingsincident voordoet, kan een datalek ontstaan. Denk daarbij aan het kwijtraken van een USB-stick, de diefstal van een laptop of een inbraak door een hacker. Datalekken kunnen ook ontstaan tijdens het mailen. Denk hierbij aan het invoeren of selecteren van een verkeerd emailadres, het versturen van een verkeerde bijlagen, het toevoegen van een mailinglijst in de CC in plaats van de BCC, etc. Verizon, een van de grootste communicatietechnologie bedrijven in de wereld, brengt met het Data Breach Investigation Report in beeld dat een deel van de beveiligingsincidenten in de gezondheidssector is terug te brengen tot menselijke fouten ('miscellaneous errors'). Denk hierbij aan verkeerde adressering, het publiceren van vertrouwelijke informatie op openbare websites of het onveilig beschikbaar stellen van persoonlijke of medische data. Andere belangrijke oorzaken zijn misbruik door medewerkers binnen de organisatie en verlies of diefstal. Onderstaande figuur geeft dit schematisch weer.

FREQUENTIE VAN DATABLOOTSTELLING

Verdeeld naar oorzaak patronen (Verizon, 2015)



2.2 Aanpak

E-mail is een veel gebruikte manier om gegevens uit te wisselen, waardoor veilig e-mailen erg belangrijk is. Vanwege de risico's die optreden bij het gebruik van e-mail, worden in deze vergelijking zowel eisen gesteld aan de gebruiker(functionaliteit) als aan de techniek/infrastructuur. Er zijn verschillende diensten beschikbaar die daarin ondersteunen. Deze vergelijking richt zich op de functionaliteiten van de diensten die bij beogen te dragen aan het vermindering van datalekken. Eerst bespreken we de globale opzet en werking van de oplossingen uit onze vergelijking, vervolgens de functies die beogen bij te dragen aan verkleining van het risico op datalekken. Daarna wordt de implementeerbaarheid en het gebruiksgemak besproken. We sluiten af met de kosten en besparingen van de individuele diensten.

DEEL 1. DE MATE WAARIN DIENSTEN VOOR VEILIGE MAIL BIJDRAGEN AAN HET VERMINDEREN VAN HET RISICO OP DATALEKKEN.

Dit rapport onderscheidt een aantal dimensies waarin datalekken kunnen optreden in e-mailverkeer. Deze dimensies zijn:

- Signalering gevoelige content
- Signalering mogelijke adresseerfouten (verkeerde ontvanger, te veel ontvangers)
- Bescherming tegen hacken tijdens verzending
- Verzekering dat alleen de ontvanger toegang heeft tot het bericht (2-factor authenticatie)
- Bescherming na verzenden (terugtrekken berichttoegang, beperken bewerkingsmogelijkheden)
- Bijdrage aan bewustwording omtrent datalekken in organisatie
- Beschikbaarheid van logginginformatie

We geven voor elke dimensie aan wat het belang is en illustreren dit belang bij een aantal dimensies met een *use case* (praktijkvoorbeeld). Vervolgens geven we per leverancier aan op welke manier deze de dimensie invult. In een samenvattend overzicht staan de scores op alle dimensies per leverancier.

DEEL 2. IMPLEMENTEERBAARHEID EN GEBRUIKSGEMAK.

Een veilige mailoplossing moet idealiter voor alle zorgorganisaties bruikbaar zijn. Ook is het belangrijk dat de dienst ondersteunend is aan de communicatie in de dagelijkse praktijk en laagdrempelig is voor verzender en ontvanger. De mate van gebruiksgemak voor zowel zorgverleners als de cliënt geven we per leverancier weer in een tabel voor zowel verzenders die de dienst gebruiken, ontvangers die de dienst gebruiken en ontvangers die de dienst (nog) niet gebruiken. Deze aspecten behandelen we in het tweede deel.

DEEL 3. DE KOSTEN EN BESPARINGEN VOOR ZORGINSTELLINGEN DIE EEN VEILIGE MAILOPLOSSING WILLEN IMPLEMENTEREN.

Het derde deel van dit rapport gaat in op de business case van de oplossingen van de leverancier. We brengen eerst de initiële kosten (bv. installatie, implementatie) en de structurele kosten (bv. abonnementskosten) in kaart en vervolgens de mogelijkheden voor besparingen.

2.3 Conclusie

Op basis van de mate waarin de bovengenoemde delen geven we in de conclusie een samenvatting van de bevindingen.

3. Opzet en werking van diensten voor veilige mail

Dit deel beschrijft vier diensten in de markt ten behoeve van veilige mail. KPN Secure Mail (ook bekend als 'KPN E-zorg') en HPE SecureMail (ook bekend als Voltage) zijn bekende dienstverleners in de zorgwereld. Sophos SPX en ZIVVER zijn nieuwe toetreders tot de markt. Hieronder geven we de diensten weer op basis van **de visie/het perspectief van de leverancier.**

3.1 KPN Secure Mail Premium (E-Zorg)

KPN Secure Mail biedt deelnemers aan de zorgketen – van specialist tot huisarts en van patiënt tot mantelzorger – een oplossing voor het onderling beveiligd e-mailen.

De dienst kenmerkt zich door:

- **Het waarborgen van de vertrouwelijkheid en integriteit van patiënt- en zorggegevens.** Zowel het transport als de opslag van informatie wordt beveiligd. Dat gebeurt binnen de eigen infrastructuur van KPN en niet op het openbare internet. Daarom wordt de dienst aangeboden binnen de KPN ZorgCloud; de besloten zorginfrastructuur van KPN. Berichten kunnen veilig direct bij ZorgCloud gebruikers afgeleverd worden of bij gebruikers van aangesloten/gekoppelde netwerken, gemeentes of bureau jeugdzorg. De aansluiting op de ZorgCloud gaat via een E-zorg-verbinding (eerstelijns zorginstellingen en zorgverleners) of een KPN ZorgConnect-verbinding (tweedelijns zorginstellingen en zorgverleners).
- **Gebruiksvriendelijkheid.** Omdat informatieveiligheid in belangrijke mate een kwestie van menselijk gedrag is, is KPN Secure Mail gebruiksvriendelijk. Medewerkers kunnen gebruik blijven maken van hun vertrouwde e-mailprogramma en hoeven hun mailgedrag dus niet te veranderen. Ook de webportal is eenvoudig in gebruik.
- **Eenvoudige implementatie.** Implementatie van KPN Secure Mail binnen de organisatie is eenvoudig. De toepassing werkt met veelgebruikte e-mailprogramma's en er is geen additionele software nodig. De organisatie kan zelf bepalen of alle mail automatisch veilig wordt verzonden, of dat er keuze is tussen het verzenden van een 'veilig' en een 'normaal' mailbericht. Niet-professionele gebruikers (cliënten, mantelzorgers etc.) maken gebruik van KPN Secure Mail via een webportal.
  Medewerkers kunnen mailberichten en bijlagen vanuit hun eigen e-mailadres/domein en e-mailprogramma versturen naar de ontvanger. Als de ontvanger aangesloten is op de KPN ZorgCloud wordt het bericht van de medewerker afgeleverd in zijn reguliere e-mailprogramma. Is de ontvanger niet aangesloten op de KPN ZorgCloud, dan krijgt hij een notificatie in zijn reguliere e-mailprogramma. Via een link kan het e-mailbericht vervolgens in een beveiligd webportal worden bekeken.

KPN Secure Mail waarborgt de vertrouwelijkheid en de integriteit van patiënt- en zorggegevens door zowel transport als de opslag van informatie te beveiligen. De visie van KPN is dat de afzender die gebruik maakt van de dienst zelf verantwoordelijk is voor de informatie die hij/zij verstuurt.

3.2 HPE SecureMail (Voltage)

HPE SecureMail is een veilig mail-systeem dat voldoet aan de regelgeving en eenvoudig integreert met bestaande systemen in een organisatie. De meeste traditionele versleutelingssystemen gebruiken meerdere afleveringsmethoden, dat resulteert in veiligheidsrisico als een bericht wordt gesplitst. Veel voorkomende problemen hierbij zijn: incompatibiliteit, verschillende inboxen, geblokkeerde of verlopen links en geblokkeerde toegang tot contacten. HPE SecureMail biedt een oplossing voor deze problemen door end-to-end versleutelingse-mail voor desktop PC, cloud en mobiele apparaten.

HPE SecureMail kenmerkt zich door:

- **Versleuteling van data en attachment.** HPE SecureMail versleutelt data en attachments zodat bij een datalek de gecodeerde inhoud geen waarde heeft voor de aanvaller. Bijlagen worden opgeslagen op interne servers, geen externe servers van derden.
- **HPE-Identifier Based Encryption.** Het onderliggende key management systeem is een belangrijke factor voor de prestaties en de kwaliteit van de ervaring van een veilige e-mailsysteem. Met behulp van op standaarden gebaseerde HPE-Identifier Based Encryption (IBE) kunnen beveiligde berichten naar elke ontvanger worden gestuurd, zonder dat de ontvanger speciale maatregelen hoeft te nemen.
- **Decryptie.** HPE SecureMail maakt decryptie op desktop, web en mobiel mogelijk, door zowel interne als externe gebruikers en ondersteunt het scannen en filtering voor alle inkomende en uitgaande e-mail.
- **Archivering en zoekfuncties.** HPE SecureMail biedt meerdere opties voor het interne supervisory control en voor de archivering van beveiligde e-mail. Met de mogelijkheid te indexeren, zoeken, bekijken en ontdekken, vereenvoudigt HPE SecureMail reacties op verzoeken tijdens de audits, onderzoeken en rechtszaken.
- **Integratie.** HPE SecureMail integreert naadloos met e-infrastructuur zoals anti-virus, anti-spam, content filtering en e-mailarchieven.
- **Flexibele inzetoptie.** HPE SecureMail ondersteunt on-premise (op locatie), in de cloud of bij hybride implementaties. Dit geldt ook voor e-maildiensten in de cloud, zoals Office 365.

3.3 Sophos SPX: SPX e-mail encryption

SPX e-mailencryptie biedt een werkzaam alternatief ten opzichte van 'traditionele encryptie-oplossingen, die vaak lastig te beheren zijn en de werkwijze van een organisatie kunnen verstoren. Het inschakelen van SPX e-mailencryptie kan actief door op de encryptieknop te drukken of door de tag 'Vertrouwelijk' te activeren, maar ook passief door middel van de ingestelde encryptierichtlijnen. Sophos SPX heeft een set richtlijnen voor health care, maar deze zijn ook instelbaar door de organisatie zelf en aan te passen naar eigen wensen. De oplossing controleert automatisch op de aanwezigheid van e-mailadressen, woorden en bijlagen en verstuurt deze – indien aanwezig – encrypted.

De oplossing leidt ertoe dat intern zonder versleuteling kan worden gemaild en dat externe e-mails encrypted worden verzonden. De verzender kan het wachtwoord voor het ontsleutelen van de versleutelde e-mails handmatig via een sms toezenden. Ook is het mogelijk om vooraf een vast wachtwoord per e-mailadres te definiëren. Sophos SPX heeft nog geen werkzaamheden in de zorg, maar biedt al wel een set van business rules specifiek voor de zorg.

3.4 ZIVVER

ZIVVER gaat uit van de filosofie dat het grootste risico niet zit in de veiligheid van de overdracht (al moet die zeker op orde zijn), maar in menselijke fouten. Met ruim 30% zijn menselijke fouten volgens ZIVVER de belangrijkste oorzaak van datalekken in de zorg. Van deze fouten is 'verkeerde adressering', bijvoorbeeld het per ongeluk selecteren van de verkeerde ontvanger, de grootste oorzaak. ZIVVER beoogt deze belangrijke oorzaak van datalekken te voorkomen.

Daarmee wil ZIVVER zich onderscheiden van sommige andere aanbieders die zich volgens ZIVVER vooral richten op encryptie. Door middel van encryptie voorkom je in de visie van ZIVVER menselijke fouten niet en kun je de consequenties van de fouten niet ondervangen. Verder biedt ZIVVER zogenaamde audit-trails, waarmee een organisatie inzicht krijgt in het communicatiegedrag van haar medewerkers. Hiermee kunnen (mogelijke) datalekken worden geanalyseerd.

In haar oplossing hanteert ZIVVER de volgende uitgangspunten:

- **Het bieden van een gebruikersvriendelijke oplossing.**
  ZIVVER wil dat een oplossing voor verzender en ontvanger aantrekkelijk is om te gebruiken. Dit geldt zowel voor de verzender als voor de ontvanger. Ook cliënten/patiënten van zorginstellingen kunnen ZIVVER installeren en moeten hetzelfde gebruiksgemak kunnen ervaren. Gevoelige informatie wordt beveiligd verzonden en voor de ontvanger automatisch ontsleuteld en ervaren als een normaal bericht. Eindgebruikers die ZIVVER niet als plug-in in zijn mailprogramma wil installeren, ontvangt een link die toegang geeft tot de eigen applicatie van ZIVVER, welke werkt op elke smartphone, tablet of pc.
- **Het bieden van een integrale oplossing.**
  ZIVVER wil bescherming, veiligheid en controle bieden. ZIVVER wil zich in eerste instantie richten op het beschermen van de verzender tegen het maken van een fout. ZIVVER controleert bijvoorbeeld of de inhoud van het bericht / de bijlagen gevoelig is, of de ontvanger logisch is en welke meldingen of veiligheidsmaatregelen (versleuteling, 2-factor authenticatie, etc.) het best passen bij de situatie. ZIVVER waarschuwt ook bij riskant gebruik van geadresseerden. ZIVVER geeft daarnaast beveiliging door gebruik van een versleutelde verbinding en versleutelde opslag, zo veel mogelijk met 2-factor authenticatie. Ten derde informeert ZIVVER bij risicovolle verzending, geeft monitoring en biedt de mogelijkheid om berichten terug te trekken.

ZIVVER is een startend bedrijf dat sinds kort actief is in de gezondheidszorg.

4. Reductie van risico op datalekken

Veiligheid is niet binair. Het is niet 'aan' of 'uit', 'goed' of 'slecht'. **Beter is het om veiligheid voor te stellen als een oplopende schaal.** De kenmerken van een veiligheidsoplossing zorgen er samen voor of een dienst hoog of laag scoort op de veiligheidsschaal. In dit onderdeel onderscheiden we zeven dimensies die relevant zijn bij de beoordeling van de mate van veiligheid. We bespreken steeds welk aspect van veiligheid de dimensie inhoudt, beoordelen de verschillende diensten en geven in een aantal gevallen een illustratie aan de hand van een of meer praktijkvoorbeelden. Het onderdeel sluit af met een algemene conclusie, waarin we per dienst aan elke dimensie een veiligheidsscore geven.

4.1 Signalering gevoelige content

Simpel gezegd: **'Mag dit bericht met de huidige inhoud worden verstuurd en is het nodig een bericht te beveiligen?'**

Heel vaak is het niet nodig om een e-mail beveiligd te versturen. Als de inhoud daar echter aanleiding toe geeft, is het van groot belang dat beveiliging wel wordt toegepast, of zelfs dat het bericht (in deze vorm) niet wordt verstuurd.

We zien bij diensten op deze dimensie:

- **Geen signalering gevoelige content** (gebruiker moet handmatig kiezen voor veilige verzending)
- **Aanname altijd gevoelige content** (beveiliging staat standaard aan)
- **Actieve signalering** op basis van inhoud van bericht en/of bijlagen (beveiliging staat aan als nodig).

Beveiliging 'standaard aan' klinkt zeer veilig, maar dit model kent ook nadelen. Ontvangers die handelingen moeten verrichten voor het openen van een beveiligd bericht, moeten dit ook doen als de inhoud van bericht deze handelingen helemaal niet rechtvaardigen. Dat kan leiden tot weerstand tegen het gebruik van deze oplossing. Verzenders kunnen als gevolg van deze weerstand voor andere mailoplossingen kiezen (bijvoorbeeld hun privémail) als zij menen dat de inhoud van een bericht niet gevoelig is. Hierdoor verliezen organisaties zicht op en regie over informatie-uitwisseling en ligt de beoordeling van de gevoeligheid van een bericht volledig bij de verzenders zelf. De relay oplossingen anderzijds, maken het juist mogelijk dat binnen de aangesloten domeinen standaard zonder versleuteling (dwz met automatische ontsleuteling) wordt gemaild. Dit leidt tot gebruiksgemak, echter zo kan vertrouwelijke content ook binnen de relay bij onbedoelde ontvangers terecht komen.

	TYPE SIGNALERING	TOELICHTING
KPN Secure Mail Premium	Geen signalering gevoelige content of aanname altijd gevoelige content (keuze organisatie).	Oplossing kijkt niet naar inhoud e-mail in verband met privacy overwegingen. Organisatie kan per gebruikersgroep kiezen voor aan of uit zetten van de oplossing.
HPE SecureMail	Actieve signalering bij externe mail leidt tot toepassing van encryptie bij verzending.	Signalering van woorden in mailinhoud.
Sophos SPX SPX e-mail encryption	Actieve signalering bij interne en externe mail leidt tot toepassing van encryptie bij verzending.	Signalering van woorden in mailtekst en inhoud van bijlagen + signalering van ontvangende maildomeinen.
ZIVVER	Actieve signalering bij interne en externe mail leidt tot waarschuwing voor verzending en toepassing van encryptie bij verzenden.	Geeft een waarschuwing over de gevoelige inhoud voorafgaand aan verzending. Signalering van woorden in mailtekst en inhoud bijlagen en relatie met ontvanger. Ook kan verzending op basis hiervan worden geblokkeerd of alleen na toestemming plaatsvinden.

Een use case van een recent datalek uit de praktijk illustreert de wijze waarop en mate waarin diensten bijdragen aan het voorkomen van dit type datalekken.

Casus 1: HRM-gegevens

Er is een mail met Excel-bestand gestuurd aan de leidinggevenden, ook bestemd voor de leidinggevenden, bestaande uit meerdere tabbladen. In een van de tabbladen staat informatie over een medewerker die niet voor anderen (ook niet voor de leidinggevenden) bestemd is.

⊖ **KPN SECURE MAIL - voorkomt het datalek niet**

KPN Secure Mail had dit bericht zonder waarschuwing beveiligd afgeleverd bij de ontvangers. Het datalek was niet voorkomen omdat de dienst niet beschikt over signalering van gevoelige content. Dit in verband met privacy overwegingen. Toepassing van encryptie zou niet plaatsvinden en zou ook niets bijdragen, omdat de beoogde ontvangers dan alsnog toegang zouden kunnen krijgen.

⊖ **HPE SECURE MAIL - voorkomt het datalek niet**

HPE Secure Mail had dit bericht in alle gevallen zonder waarschuwing bezorgd bij de ontvangers. Het DLP-filter kijkt alleen naar de mailtekst, niet in bijlagen en doet dat alleen bij mail die de organisatie verlaat.

⊕ **SOPHOS SPX - voorkomt het datalek mogelijk**

Het DLP filter van Sophos kijkt zowel naar de mailtekst als naar de inhoud van bijlagen, zowel bij interne als externe mail. Toepassing van encryptie zou dus wel plaatsvinden, maar niets bijdragen, omdat de beoogde ontvangers dan alsnog toegang zouden kunnen krijgen. Sophos kan wel zo worden ingesteld dat mails met vooraf bepaalde vertrouwelijke inhoud in quarantaine worden geplaatst of met extra onderwerpitems worden afgeleverd. Deze configuratie bij HRM-content voorkomt in dit geval weliswaar het datalek maar kan organisatiebreed tot vertraging van andere werkprocessen of work arounds leiden, waardoor deze instelling minder gebruiksvriendelijk is.

ZIVVER - voorkomt het datalek mogelijk

Indien de business rules van ZIVVER juist waren ingesteld (bijvoorbeeld waarschuwing/blokkering bij aanwezigheid bepaalde woorden in bijlage) was de gebruiker - voordat de e-mail was verzonden - er op geattendeerd dat de bijlage vertrouwelijke woorden bevat. Doordat de gebruiker hierop was gewezen, had hij/zij mogelijk het versturen van dit document met deze inhoud heroverwogen. De preventiewerking van ZIVVER had het datalek mogelijk kunnen voorkomen.

4.2 Signalering adresseerfouten

Simpel gezegd: **'Gaat deze mail naar de juiste persoon/personen?'.**

Veel vormen van technische beveiliging helpen niet tegen een vaak voorkomende fout: een adresseerfout. Wie met maximale encryptie en een verplichte 2-factor informatie naar de verkeerde persoon stuurt, zorgt er alleen maar voor dat die verkeerde persoon de informatie heel veilig ontvangt. Wie meerdere ontvangers in het aan-: of cc:-veld plaatst, kan er onbedoeld voor zorgen dat ontvangers van elkaar iets te weten komen dat niet gedeeld mocht worden. Sommige veilige maildiensten zien deze fouten als een verantwoordelijkheid van de verzender. Anderen hebben functies die beogen medewerkers te helpen om deze fouten te voorkomen.

	TYPE SIGNALERING	TOELICHTING
KPN Secure Mail Premium	Geen	Richt zich op veilig transport en ontvangst
HPE SecureMail	Geen	Richt zich op veilig transport en ontvangst met instelbare handmatige of automatische 2-factor
Sophos SPX SPX e-mail encryption	Geen	Richt zich op veilig transport en ontvangst met instelbaar handmatige 2-factor
ZIVVER	Actieve signalering	Signaleert niet-zakelijke mailextenties, meerdere ontvangers en mismatch tussen type content en type ontvanger. Content afhankelijk handmatige of automatische 2e factor.

Twee use cases van recente datalekken uit de praktijk illustreren de wijze waarop en mate waarin diensten bijdragen aan voorkomen van dit type datalekken.

Casus 1: Verkeerde e-mailadres

Een zorgorganisatie blijkt gevoelige medische gegevens naar een toeleverancier (IT-bedrijf) te hebben gestuurd. Het gaat onder meer om de diagnose en gebruikte medicatie van een patiënt. Een medewerker stuurde informatie in een onversleutelde e-mail naar een algemeen e-mailadres van het bedrijf. Het bericht volgt op een overleg tussen artsen en werd per ongeluk aan het bedrijf geadresseerd.

KPN SECURE MAIL - kans op datalek blijft bestaan

Met deze oplossing wordt het bericht wel veilig afgeleverd maar zou het datalek niet zijn voorkomen. De mail zou bij de standaard instellingen, beveiligd op een webportal aan de IT-leverancier door middel van een wachtwoord beschikbaar zijn gesteld. Indien de ontvanger zich er niet van bewust is dat de mail niet voor hem bedoeld is, zal hij/zij via een link in het notificatiebericht een account aan kunnen maken en na het lezen ontdekken dat deze informatie niet voor hem/haar is bedoeld.

HPE SECUREMAIL - voorkomt het datalek mogelijk

Indien gebruik wordt gemaakt van de veilig verzendknop of indien het filter juist (bijvoorbeeld encryptie bij info@ adressen) is ingesteld wordt de mail versleuteld verstuurd. Als HPE SecureMail vervolgens zo was ingesteld dat de verzender handmatig een 2-factor wachtwoord naar de ontvanger moest sturen, was het datalek mogelijk voorkomen, omdat de medewerker waarschijnlijk is niet ook per ongeluk de 2-factor naar de verkeerde ontvanger stuurt. Als HPE SecureMail zo is ingesteld dat de 2-factor automatisch wordt aangeboden, blijft het datalek bestaan. Het systeem zal de 2-factor namelijk wel aanbieden aan de verkeerd ingevoerde ontvanger indien de gegevens van deze ontvanger bekend zijn bij de organisatie. De ontvanger kan vervolgens het bericht ongehinderd openen om er vervolgens achter te komen dat de inhoud niet voor hem bedoeld is.

SOPHOS SPX - voorkomt het datalek mogelijk

Als de organisatie over Sophos SPX beschikt, kan de medewerker in Outlook de functie 'secure e-mail' activeren. Vervolgens wordt elke e-mail die naar een e-mailadres buiten de organisatie is gericht, versleuteld verstuurd. Dit is enkel te openen met een wachtwoord. De mail wordt automatisch geencrypt indien deze een bijlage (Word, Excel, Pdf) of woorden bevat die zijn opgenomen in de encryptierichtlijnen. Indien de encryptierichtlijnen goed waren ingesteld, was de mail versleuteld naar het IT-bedrijf verstuurd. Als Sophos SPX vervolgens zo was ingesteld dat de verzender handmatig een 2-factor wachtwoord naar de ontvanger moest sturen, was het datalek mogelijk voorkomen, omdat niet aannemelijk is dat de medewerker ook per ongeluk de 2-factor naar de verkeerde ontvanger stuurt.

ZIVVER - voorkomt het datalek waarschijnlijk

ZIVVER attendeert de gebruiker eerst door meldingen in Outlook real time op gerichtheid aan een onbekend e-mailadres en of de e-mail/bijlage kenmerken bevat die vertrouwelijkheid vereisen. Tevens is er actieve monitoring op de match tussen inhoud en ontvanger. In bovengenoemde casus zou de medewerker die de mail aan het IT-bedrijf verstuurde, bij de juiste instellingen, al tijdens het opstellen van de mail geattendeerd worden op het gebruik van woorden die vertrouwelijk zijn en ook erop zijn gewezen dat het e-mailadres – mede in relatie tot de inhoud van de mail en bijlage – onbekend/ waarschijnlijk niet correct is. Dit had het datalek mogelijk voorkomen. Daarnaast kan, hoewel minder gebruiksvriendelijk, bij ZIVVER contextueel worden ingesteld dat de 2-factor van de ontvanger handmatig door de zender, als extra controle, moet worden ingevoerd.

Casus 2: Mail naar meer ontvangers (zichtbaar in *aan*: en *cc*:)

Een medewerker van een zorgorganisatie verzond een e-mail aan een groep cliënten. Omdat cliënten elkaars e-mail niet mogen ontvangen zouden deze e-mailadressen in de 'BCC' moeten zijn ingevoerd, echter zijn deze abusievelijk in de 'CC' gezet, waardoor de cliënten ook elkaars e-mailadressen ontvingen en daarmee bekend werd wie cliënt was bij de betreffende organisatie.

KPN SECURE MAIL - voorkomt het datalek niet

Geadresseerden kunnen dit bericht in alle gevallen openen en kunnen vervolgens ook de CC:-e-mailadressen zien van de andere personen aan wie de mail gericht was. Dit incident had niet kunnen worden voorkomen met KPN Secure Mail.

HPE SECUREMAIL - voorkomt het datalek niet

Het veld BCC: wordt niet ondersteund door HPE SecureMail omdat het systeem dan niet kan bepalen naar welke adressen de sleutels moeten worden verzonden. Indien dit wel mogelijk was, kunnen geadresseerden dit bericht in alle gevallen openen en vervolgens ook de CC:-e-mailadressen zien van de andere personen aan wie de mail gericht was. HPE SecureMail had dit datalek niet kunnen voorkomen.

SOPHOS SPX - voorkomt het datalek mogelijk

Sophos had de email bij ontvangers afgeleverd, maar biedt de mogelijkheid om mail headers te strippen waardoor e-mail adressen die in de Aan: of CC: staan onzichtbaar gemaakt kunnen worden. Dit incident had bij de juiste instelling kunnen worden voorkomen met Sophos SPX.

ZIVVER - voorkomt het datalek waarschijnlijk

ZIVVER informeert deze medewerker indien hij/zij de adressen invoert, dat het ongebruikelijk is om meer dan # (door organisatie in te stellen) e-mailadressen in het Aan: of CC: veld te hebben. Doelstelling van de attendering is om bewustzijn en waakzaamheid bij de medewerker te creëren. De medewerker krijgt het advies om ontvangers individuele mails te sturen of de adressen (automatisch door ZIVVER) in de BCC te verplaatsen. Ook kan een organisatie het verzenden van de mail in dit geval blokkeren. Mits de business rules goed zijn ingesteld had ZIVVER door de medewerker te attenderen het datalek waarschijnlijk voorkomen.

4.3 Bescherming tegen hacken tijdens verzending

Simpel gezegd: **'Kan een kwaadwillende meekijken?'.**

De veilige mailoplossingen zorgen voor een domein waarin onderling berichtenverkeer van het internet is afgeschermd of passen encryptie toe waarbij alleen verzender en ontvanger de sleutel hebben. De oplossing die werkt met een domein (KPN ZorgCloud) heeft ook te maken met ontvangers die buiten dit domein vallen. Deze berichten dienen door middel van een wachtwoord te worden gelezen op een portal (KPN).

	TYPE BESCHERMING	TOELICHTING
KPN Secure Mail Premium	Bescherming tegen hackers binnen de federative relay/KPN ZorgCloud. Toegang tot de portal voor ontvangers buiten de relay is ook te verkrijgen door hackers die toegang hebben verkregen tot de ontvangende persoonlijke mailbox.	≫ Automatische decryptie binnen relay ≫ Buiten relay toegang via portal met wachtwoord
HPE SecureMail	Encryptie met 2-factor	Identity based end-to-end encryptie, inclusief 2-factor authenticatie
Sophos SPX **SPX e-mail encryption**	Encryptie met 2-factor	Encryptie, inclusief 2-factor authenticatie
ZIVVER	Encryptie met 2-factor	Asymmetrische encryptie met automatische ontsleuteling voor ZIVVER gebruikers in plugin en/app/ of online. Ontsleuteling met 2-factor voor niet-ZIVVER gebruikers

De situatie bij KPN Secure Mail verdient wat extra toelichting. Deze oplossing geeft bescherming tegen hackers binnen de KPN ZorgCloud. Dit is een van het openbare internet afgesloten omgeving waarbij de emaildomeinen van een groot aantal vertrouwde zorg- en andere organisaties zijn aangesloten en onderling beveiligd kunnen mailen. Voor ontvangers die niet zijn aangesloten bij de KPN ZorgCloud is een andere oplossing gekozen: ontvangers maken een account aan voor een webportal waarna zij het bericht kunnen lezen. Dit leidt tot een veiligheidsrisico omdat ook het risico bestaat dat een meelezende hacker een account aan kan maken als hij het allereerste notificatiebericht onderschept en/of zich toegang weet te verschaffen tot de persoonlijke mailbox van de ontvanger. De visie van KPN is echter dat de beveiliging van de persoonlijke mailbox en de verbindingen tot de mailbox de verantwoordelijkheid zijn van de ontvanger.

4.4 Verzekering dat alleen de ontvanger toegang heeft tot het bericht

Simpel gezegd: **'Kan iemand anders met toegang tot de mailbox van de ontvanger ook toegang krijgen?'**

Sommige veilige mailoplossingen zorgen ervoor dat (als de inhoud van het bericht dit rechtvaardigt) alleen de gekozen ontvanger toegang tot het bericht heeft. Dit kan bijvoorbeeld door een 'tweede factor' verplicht te stellen. Dit kan zijn een sms-bericht per bericht, een afgesproken wachtwoord, of authenticatie met een account waarvan het wachtwoord nooit via e-mail wordt gedeeld. Andere leveranciers hangen daarentegen de mening aan dat beveiliging van de persoonlijke e-mailbox de verantwoordelijkheid van de ontvanger.

Het RZCC volgt hierin het advies van NICTIZ. NICTIZ adviseert zorginstellingen die medische gegevens met patiënten delen via e-mail om in die communicatie 2-factor authenticatie te gebruiken met een unieke code per bericht (via sms of een OTP-code via een app). Zie "Handreiking Patientauthenticatie" van Nictiz (2013).

	TYPE 2-FACTOR AUTHENTICATIE	TOELICHTING
KPN Secure Mail Premium	Geen	Binnen de KPN ZorgCloud is de mailbox gekoppeld aan de zakelijke mailbox/ werkplek. Buiten de cloud kan de ontvanger bij eerste maal inloggen in het webportaal zelf een account aanmaken.
HPE SecureMail	Optioneel. Wachtwoord handmatig of automatisch te versturen door ontvanger.	Instelbaar is dat de verzender zelf een wachtwoord bepaald dat hij/zij op een andere wijze dan mail aan de ontvanger beschikbaar moet stellen. Ook kan het systeem automatisch een 2-factor authenticatie via SMS versturen.
Sophos SPX: SPX e-mail encryption	Wachtwoord handmatig te versturen door ontvanger.	Instelbaar is dat de verzender van Sophos een token/code krijgt die hij/zij op een andere wijze dan mail aan de ontvanger beschikbaar moet stellen. Toepassing 2-factor authenticatie kan op basis van vertrouwelijke inhoud, medewerker of afdeling worden ingesteld.
ZIVVER	Standaard aan maar uit te zetten. Wachtwoord automatisch via SMS, handmatig via ander kanaal of automatisch via persoonlijk ZIVVER account van ontvanger.	ZIVVER stuurt (na handmatige invoer nummer of automatisch) een code via SMS, of verzender stelt zelf een wachtwoord in en deelt dat via een ander communicatiemiddel met ontvanger. De ontvanger met een ZIVVER account kan zich met dat account (evt nog beschermd met extra 2-factor) authentiseren. Op basis van context/content wordt toepassing 2-factor (niet/ automatisch/ handmatig) bepaald.

4.5 Bescherming na verzenden

Simpel gezegd: **‘Welke invloed heb ik als verzender op mijn bericht na verzending?’.**

Sommige veilige mailoplossingen bieden ook na de druk op de verzendknop nog de mogelijkheid om de toegang tot berichten en de gebruiksmogelijkheden van verstuurde documenten te beïnvloeden. Dit draagt alleen bij aan het voorkomen van datalekken als de verkeerde ontvanger de ontvangen gegevens (mail) nog niet (handmatig) heeft geopend. Daarnaast bieden sommige veilige mailoplossingen aanvullende bescherming zoals pdf-conversie, kopieer- en printbescherming. Deze bescherming blijft bestaan, ook als de ontvanger de gegevens (handmatig) heeft geopend.

	TYPE BESCHERMING	TOELICHTING
KPN Secure Mail Premium	Geen	KPN Secure Mail biedt geen functionaliteit waarmee verzonden e-mails teruggetrokken of aangepast kunnen worden.
HPE SecureMail	Kan op key server worden ingetrokken.	De verzender heeft de mogelijkheid om de sleutel tot het bericht indien deze nog niet is opgehaald door de ontvanger in te trekken, waardoor dit niet meer te openen is.
Sophos SPX SPX e-mail encryption	Het wachtwoord van de ontvanger kan worden gewist.	De verzender heeft de mogelijkheid om de sleutel tot het bericht indien deze nog niet is opgehaald door de ontvanger in te trekken, waardoor dit niet meer te openen is. Ook kan het aantal dagen worden ingesteld waarbinnen gelezen en geantwoord kan worden.
ZIVVER	Actieve toegangscontrole, office-pdf-omzetting en toevoegen watermerken.	Verzender kan toegang tot een bericht na instelbaar aantal dagen laten verlopen en ad-hoc terugtrekken, ook als het al gelezen is. Verder zijn watermerken, kopieer- en printbescherming in te stellen.

4.6 Bijdrage aan bewustwording omtrent datalekken in organisatie

Simpel gezegd: **'Welke bijdrage levert het product aan meer bewustzijn in mijn organisatie over informatiebeveiligingsrisico's?'.**

Het lijkt aantrekkelijk om via de techniek zoveel mogelijk risico's op datalekken in te dekken. Toch zal het altijd belangrijk blijven dat ook medewerkers zich bewust zijn van risico's. Een van de eisen die de wetgever daarom stelt, is dat organisaties aantoonbaar werken aan de ontwikkeling van het bewustzijn over datalekken bij medewerkers. Sommige oplossingen zien de bewustwording als een verantwoordelijkheid van de medewerker en kiezen ervoor om deze niet actief te beïnvloeden, zodat zij leren van fouten. Andere veilige diensten attenderen medewerkers juist wel op risico's, bij voorkeur op een moment dat zij nog zelf kunnen ingrijpen en op een manier die hun werkproces niet (onnodig) verstoord.

	TYPE BIJDRAGE	TOELICHTING
KPN Secure Mail Premium	De verzender is zelf verantwoordelijk voor de informatie die hij/zij verstuurt. Er is optioneel een veilige mail-knop zichtbaar. Deze heeft ook een signaalfunctie.	Oplossing werkt verder grotendeels op de achtergrond ter bevordering van gebruiksgemak en acceptatie. Het draagt daardoor beperkt bij aan bewustwording gebruikers.
HPE SecureMail	Er is optioneel een veilige mail-knop zichtbaar. Deze heeft een signaalfunctie. (Optioneel) instellen 2-factor bij encryptie.	Oplossing werkt verder grotendeels op de achtergrond en draagt daardoor beperkt bij aan bewustwording gebruikers. 2-factor leidt door extra handelingen verzender tot bewustwording.
Sophos SPX SPX e-mail encryption	Er is een veilige mailknop zichtbaar. (Optioneel) instellen 2-factor bij encryptie.	Verzenders krijgen van de Sophos key generator t.b.v. ontvanger een wachtwoord toegestuurd via mail. In deze mail kan de organisatie zelf waarschuwingen opnemen (vrije tekst). Als gebruikers 2-factor moeten instellen bij encrypted mails en dat gebeurt inclusief uitleg over de noodzaak, kan dit ook bijdragen aan bewustwording.
ZIVVER	Geeft risico's weer en beoogt gebruikers daardoor te leren de risico's te kennen.	Geeft, voorafgaand aan verzending, actief meldingen over risico's. De dienst is niet zichtbaar totdat actieve screening van de inhoud of ontvangers daar aanleiding toe geeft of indien verzender ZIVVER zelf zichtbaar maakt.

4.7 Beschikbaarheid van logging-informatie (t.b.v. rapportage en monitoring)

Simpel gezegd: **'Kan ik ergens zien wanneer wat naar wie is verzonden?'.**

De beschikbaarheid van logginginformatie dient twee doelen: rapportage ten behoeve van verbetering en informatieverzameling bij constatering van een datalek. Sommige oplossingen beperken zich tot algemene en geageerde rapportage/logging. Andere leggen meer kenmerken van berichtenverkeer vast. Intelligente loggingsystemen kunnen zo worden ingesteld dat zij mogelijke datalekken in de logginginformatie herkennen en direct melden.

	TYPE INFORMATIE	TOELICHTING
KPN Secure Mail Premium	Metadata wordt gelogd en is beschikbaar.	Zender, afzender, verzenddatum en tijdstip verzending worden gelogd. Informatie kan worden opgevraagd. Loggingsysteem bevat geen intelligentie.
HPE SecureMail	Uitgebreide mogelijkheden voor archivering en terugzoeken.	Instelbaar op basis van wensen organisatie. Ook is er een HPE E-discovery module beschikbaar.
Sophos SPX SPX e-mail encryption	Real time dashboards en maillog (live en archief)	Veilig mailgedrag medewerkers afdelingen kan worden gemonitord. Ook rapportagemogelijkheden (grafieken, top 10's etc.). Verstuurt een melding naar medewerker/ICT-afdeling bij verzenden bericht met hoog risico op datalek.
ZIVVER	Meldingen bij mogelijke datalekken en uitgebreide logginginformatie	Verstuurt een melding bij verzenden bericht met hoog risico op datalek. Verder logging/rapportages van verzender, ontvanger, tijdstippen toegang, onderwerp, naam en type bijlagen en IP-adressen. Tevens van waarschuwingen en genomen acties.

4.8 Totaaloverzicht functionaliteiten t.b.v. voorkomen datalekken

In onderstaande tabel wordt weergegeven met welke functionaliteiten de vergeleken veilige maildiensten organisaties beogen te ondersteunen om risico's op datalekken te beperken. We scoren de functionaliteiten die de diensten aanbieden t.b.v. het voorkomen van datalekken. Deze bijdrage wordt per leverancier numeriek weer gegeven in een schaal van 1 tot 5, waarbij een dienst die veel functionaliteit biedt t.a.v. het voorkomen van een datalek het nummer 5 krijgt en een dienst die minder/geen functionaliteiten biedt nummer 2 of 1. Deze vertaling is geen harde wetenschap. Er is steeds gezocht naar een score die een redelijke weergave geeft van verschillen in prestaties.

FUNCTIES VAN DE DIENSTEN T.A.V. HET VOORKOMEN VAN DATALEKKEN

(1= beperkte of geen functies, 5=meeste functies)

	KPN SECURE MAIL	HPE SECUREMAIL	SOPHOS SPX: SPX E-MAIL ENCRYPTION	ZIVVER
Signalering content	1	2	3	5
Signalering adresseerfouten	1	2	3	5
Hack bescherming	3	4	4	5
Authenticatie	2	3	3	5
Bescherming na verzending	1	3	3	4
Bewustwording	1	3	3	5
Logging	2	4	5	5

De ene dienst beidt meer (technische) functionaliteiten dan de andere. Het belang van deze functionaliteiten is ook afhankelijk van de inbedding van de dienst in de organisatie en van het mailgedrag van de medewerkers. We trachten daarom inzicht te geven in de verschillen in visie en in technieken tussen diensten, zodat zorginstellingen bewust hun eigen keuze kunnen maken. Op het gebied van preventie van menselijke fouten (stadium voorafgaan aan het versturen) is er een duidelijk verschil in visie tussen de leveranciers. KPN richt zich (vrijwel) niet op preventie van menselijke fouten (signalering content, signalering adresseer fouten). KPN beschouwt menselijke fouten namelijk als een verantwoordelijkheid van de verzender/medewerker. Het op de achtergrond werken van de dienst wordt in deze zin juist als een kracht te zien. ZIVVER ziet menselijke fouten als een belangrijke oorzaak van datalekken en wil deze voorkomen. De dienst heeft actieve signalering van gevoelige content en van adresseerfouten als functies toegevoegd. In de visie van ZIVVER zullen deze waarschuwingen leiden tot een leerproces en bewustwording. Wat betreft het transport (hack bescherming, authenticatie) brengt KPN Secure Mail een veilige verbinding (KPN ZorgCloud) tot stand, die bescherming tegen hackers geeft. Daarbuiten zijn de risico's op hacking ten opzichte van andere diensten hoger doordat geen 2-factor authenticatie wordt toegepast. Echter ziet KPN ook beveiliging van de persoonlijke mailbox expliciet als een taak en verantwoordelijkheid van de ontvanger. HPE SecureMail, Sophos SPX en ZIVVER hebben wel 2-factor authenticatie en beogen daardoor het risico op adresseerfouten en hacking te verkleinen. Tot slot lopen ook op het punt van logging-functionaliteit (logging) de visies en functionaliteiten uiteen. KPN wil zich in verband met privacy-overwegingen beperken tot meta data. HPE, Sophos en ZIVVER geven uitgebreidere monitoringsfuncties om organisaties inzicht te geven in gedrag van veilig mailen.

5. Implementatie en gebruiksgemak

Een goede veilige mailoplossing is voor een organisatie relatief eenvoudig te implementeren en **gebruiksvriendelijk voor verzender en ontvanger**. Beide onderdelen werken we hieronder verder uit.

5.1 Wijze van implementatie

KPN Secure Mail is verhoudingsgewijs eenvoudig te implementeren voor zowel kleine als grote organisaties. Grotere organisaties kunnen hun domeinnaam aansluiten op de KPN ZorgCloud. Dit betreft hoofdzakelijk een aanpassing van de configuratie en er is geen specifieke hardware/software nodig. Door beveiligingsinstellingen en testen moet rekening worden gehouden met 2 tot 4 weken doorlooptijd. Beide oplossingen zijn voor kleine organisaties en praktijken laagdrempelig, omdat ze een hosted mail variant aanbieden. Eerstelijns zorgverleners die beschikken over een E-Zorg verbinding ontvangen twee KPN Secure Mail accounts. Sophos SPX en HPE SecureMail zijn applicaties die 'on premise' (op locatie) op centraal niveau worden geïnstalleerd. Sophos heeft ook een software-variant met eigen hardware of kan werken op basis van 'hypervisor'. Het implementeren van ZIVVER vindt enkel plaats door installatie van een plug-in in het Outlook-account van de eindgebruiker. Dit kan door de eindgebruiker zelf vrij eenvoudig worden geïnstalleerd. Voor kleine organisaties/praktijken zijn de hosted mail oplossingen van KPN Secure Mail en ZIVVER wat laagdrempeliger.

5.2 Gebruiksgemak

Een veilige mailoplossing is voor verzender en ontvanger gebruiksvriendelijk. Is dit niet het geval, dan bestaat het risico dat medewerkers uitwijken naar meer praktische alternatieven zoals post, fax, telefoon of privé-e-mail. Bij de veilige maildiensten doen de extra stappen zich voor aan de ontvangerszijde en dan vooral voor ontvangers die niet van het systeem gebruik maken. De omvangrijke cloud van KPN Secure Mail zorgt ervoor dat gebruikers onderling geen verschil merken met normaal mailen. Berichten binnen de cloud worden als veilig beschouwd en kunnen zonder extra stappen worden verstuurd en ontvangen met de eigen zakelijke mailbox. Dit geeft gebruiksgemak en vergroot de acceptatie. Hiertegenover staat dat de bescherming beperkter is: transportbeveiliging en hacken maar niet menselijke fouten en ontvangers authenticatie. KPN Secure Mail is voor derden ook vrij eenvoudig te gebruiken op webportal of op mobiele telefoon. Ook bij HPE Secure Mail, Sophos SPX en ZIVVER kunnen gebruikers onderling - met uitzondering van de waarschuwingen in het geval van ZIVVER - eenvoudig en zonder extra stappen mailen. Niet HPE/Sophos gebruikers (zoals de cliënt) krijgen de mail in pdf en dienen deze door middel van een wachtwoord te ontsleutelen, hetgeen evenals bij VE Secure e-mail, minder gebruiksgemak geeft. Gebruikers zonder ZIVVER-account kunnen mailen door in te loggen via een portal of door middel van de ZIVVER-web-app. Op deze wijze kan ook naar de toekomst toe laagdrempelig en ook mobiel worden gecommuniceerd met cliënten en patiënten. Voor HPE SecureMail, Sophos SPX en ZIVVER geldt dat ontvangers een 2-factor kan worden gevraagd. Hiervoor heeft de ontvanger een mobiele telefoon nodig of kan een wachtwoord worden afgesproken. Samenvattend brengt een cloud-oplossing weliswaar gebruiksgemak, maar zwakt deze de risico's op datalekken maar voor een deel af. ZIVVER biedt in relatie tot het beschermingsniveau de hoogste mate van gebruiksvriendelijkheid.

Daarnaast geldt voor alle leveranciers dat regionale afname van eenzelfde oplossing in alle gevallen tot een forse toename van het gebruiksgemak voor zorgorganisaties onderling leidt. Hierdoor kan tussen organisaties die hetzelfde systeem gebruiken onderling zonder extra stappen veilig worden gemaild omdat automatisch wordt ontsleuteld.

SCORES MATE VAN GEBRUIKSVRIENDELIJKHEID VAN VEILIGE MAILDIENSTEN

» (1= ontbreekt/risico en 5= best practice)

	KPN SECURE MAIL	HPE SECUREMAIL	SOPHOS SPX: SPX E-MAIL ENCRYPTION	ZIVVER
Gemak verzender	4	4	4	4
Gemak ontvanger met oplossing	5	5	5	5
Gemak ontvanger zonder oplossing	4	3	3	5

6. Kosten en besparingen veilige maildiensten

Dit deel gaat in eerste instantie in op de **prijsmodellen van de diensten**. We brengen de kosten en in beeld voor een fictieve zorgorganisatie van 400 medewerkers. Vervolgens geven we **kwalitatief de besparingen** weer die kunnen worden gerealiseerd met de dienst.

6.1 Kosten van de diensten

De in tabel 2 weergegeven kosten zijn gebaseerd op de fictieve organisatie en de informatie die de leveranciers beschikbaar stellen[1], uitgaande van een 3-jarig contract. Dit zijn echter standaard tarieven. De werkelijke kosten zijn mede afhankelijk van de specifieke situatie van de afnemende organisatie en bijvoorbeeld of de organisatie al van andere diensten van de leverancier gebruik maakt. Daarnaast geldt voor vier leveranciers dat een afname van een groter aantal accounts in regionaal verband tot (sterke) prijsreductie leidt.

WEERGAVE JAARLIJKSE KOSTEN (EXCLUSIEF BTW)

» voor de fictieve zorgorganisatie exclusief (regio) korting

Kosten	KPN Secure Mail	HPE Secure Mail	Sophos SPX	ZIVVER
Eenmalig	€ 0,-	€ 4.400,-	€,-	€ 0,-
Contract	€ 9.600,-	€ 17.230,-	€ 2.000,-[2]	€ 18.340,-
Gemiddeld[3]	€ 9.600,-	€ 18.110,-	€ 2.000,-	€ 18.340,-
Gem. Regio[4]	€ 9.600,-	€ 15.512,-	€ 1.600,-	€ 5.136,-

Opmerking: Bij afname van de Sophos-oplossing zal de levering tevens een volledige anti-spam en anti-virus licentie bevatten voor het scannen van alle inkomende en uitgaande e-mail met 2 AntiVirus engines (dual scan) van Avira en Sophos.

6.2 Besparingen

Een veilige maildienst stelt de organisatie in staat om besparingen te realiseren. Bijvoorbeeld doordat e- mail vaker en voor meer vormen van communicatie kan worden ingezet. Hierdoor ontstaat tijdwinst voor medewerker, kan frequenter worden gecommuniceerd en ook kan het aantal op te stellen en te versturen brieven en faxen worden verminderd. Tevens kan een veilige maildienst risico's op datalekken verkleinen en daarmee imagoschade en eventueel boetes voorkomen. De mate waarin bovenstaande besparingen kunnen worden bereikt hangt samen met het beveiligingsniveau en het gebruiksgemak wat de maildiensten bieden.

1. De kosten zijn in beeld gebracht op basis van de tarieven zoals ten tijde van dit onderzoek beschikbaar gesteld door de leveranciers. De specifieke omstandigheden of andere diensten die worden afgenomen door een organisatie kunnen tot belangrijke afwijkingen hierin leiden. De tarieven dienen te worden nagevraagd bij de leveranciers.
2. Sophos werkt bij een 3-jarig contract met betaling op voorhand.
3. Gemiddelde kosten per jaar gerekend over 5 jaar, waarbij de initiële investering over 5 jaar wordt afgeschreven.
4. Gemiddelde kosten bij regionale afname van minimaal 5.000 accounts. Uitgangspunt is dat optelling van accounts/regionale afname bij de leverancier mogelijk is. Dit dient nog met de leverancier te worden overeengekomen.

7. Conclusie

In dit rapport zijn door het Regionaal Zorg Communicatie Centrum vier veilige maildiensten vergeleken op hun bijdrage aan de **risicobeperking van datalekken voor zorgorganisaties**. De maildiensten zijn verder vergeleken op basis van de dimensies veiligheid, implementatie en gebruiksgemak. Daarnaast zijn kosten en mogelijke besparingen weergegeven.

We brengen in beeld dat de diensten kunnen helpen om datalekken te voorkomen door beveiliging op drie onderdelen van de e-mail: het verzenden, het transport en het ontvangen. De diensten variëren sterk in hun visie op veilig mailen. KPN Secure Mail beperkt zich bewust tot het tot stand brengen van een veilige verbinding binnen de KPN Cloud. Deze diensten beveiligen het transport van de e-mail, maar werken verder in grote mate op de achtergrond. Menselijke fouten (en de bewustwording hierover) en ontvanger authenticatie zien deze diensten nadrukkelijk als een verantwoordelijkheid van de organisatie/eindgebruiker zelf. HPE SecureMail, Sophos SPX en ZIVVER bieden door middel van 2-factor authenticatie ook extra beveiliging van aflevering van de e-mail. ZIVVER is de enige leverancier die door waarschuwing voor het verzenden ondersteunt om menselijke fouten te voorkomen.

KPN Secure Mail en ZIVVER geven het grootste gebruiksgemak voor zorgverleners onderling. KPN Secure Mail laat daarbij wel meer risico's op datalekken in stand. KPN Secure Mail en ZIVVER zijn naar de cliënt en niet-gebruikers van het systeem het meest gebruiksvriendelijk. ZIVVER en in mindere mate HPE en Sophos bieden meer functionaliteiten om datalekken tegen te gaan. Voor alle veilige maildiensten geldt verder dat een regionaal gebruik van hetzelfde systeem leidt tot een forse toename in gebruiksvriendelijkheid.

Als laatste onderdeel van deze vergelijking zijn de kosten van de veilige maildiensten aan de hand van een fictieve zorgorganisatie uiteengezet. Hoewel de werkelijke individuele kosten per organisatie door specifieke omstandigheden maatwerk kunnen zijn, zijn de standaard tarieven bij individuele afname van KPN Secure Mail lager en voor HPE SecureMail en ZIVVER hoger. Regionale afname leidt voor vrijwel alle leveranciers tot kortingen. Tegenover de investeringen die een organisatie maakt door de aanschaf van een veilige maildienst, staan ook grote besparingen. Deze besparingen komen bijvoorbeeld uit tijdswinst, vervanging van andere communicatiemiddelen en verkleining van de kans op imagoschade en boetes. De mate van besparing hangt samen met de geboden beveiliging en de gebruiksvriendelijkheid.

Concluderend hebben de leveranciers verschillende visies op veilige mail en de rol die het systeem en eindgebruiker hierin beiden (moeten) spelen. De ene dienst wil zorgorganisatie op een andere wijze ondersteunen in het voorkomen van datalekken dan de andere.

Het RZCC is van mening dat bewustwording bij de gebruiker m.b.t. het gepast omgaan met patiëntinformatie en andere privacygevoelige gegevens een groot goed is. Deze bewustwording is een wisselwerking tussen systeem en eindgebruiker. Elke zorgorganisatie dient voor zichzelf te bepalen in hoeverre zij haar medewerkers dient te faciliteren in het veilig mailen, en welke rol een veilige mail oplossing hierin kan spelen.

Deze analyse laat zien dat een gezamenlijke regionale keuze voor een veilige maildienst voordelen biedt. Regionaal gebruik leidt tot meer gebruiksgemak, aanzienlijk lagere kosten en door eenduidig gebruik tot meer veiligheid. Met de wetenschap dat de individuele afweging/best passende oplossing per afzonderlijke organisaties kan verschillen, lijkt ZIVVER momenteel een geschikte keuze voor een veilige e-maildienst. Deze dienst geeft de meest complete bescherming tegen datalekken en is voor uiteenlopende doelgroepen (zorgverleners onderling, externen en de cliënt) het meest gebruiksvriendelijk. De toegevoegde waarde ten opzichte van de andere leveranciers is primair gelegen in de preventie van een belangrijke oorzaak van datalekken: menselijke fouten en in het bewustwording/leereffect voor medewerkers en de organisatie.

RZCC
Boschdijk 769
5626 AB Eindhoven
T 040-2393000

E info@rzcc.nl
I www.rzcc.nl