Whitepaper

zivver

8 praktische oplossingen voor beter digitaal communiceren in de zorg

Voorwoord: pragmatische aanpak helpt digitale transformatie in de zorg

Digitalisering en voldoen aan altijd veranderende wet- en regelgeving zijn grote uitdagingen waar zorgorganisaties dagelijks mee worstelen. Dat is helemaal niet zo gek gezien de complexiteit van de sector. Maar ondanks die complexiteit doen we het eigenlijk zo slecht nog niet, zo blijkt uit het rapport Digital Transformation: Shaping the Future of European Healthcare van Deloitte.

Uit het onderzoeksrapport blijkt dat Nederland namelijk digitale voorloper is binnen Europa. Zo werkt in ons land maar liefst 97% van de zorgverleners met een elektronisch patiëntendossier (EPD) en ook 97% werkt met het digitaal voorschrijven van medicatie.

Wat wel een typisch Nederlands issue is, zo blijkt uit het rapport, is het delen van patiëntendata en digitale communicatie. Vaak staan privacyoverwegingen dat in de weg. Maar liefst 44% van de respondenten geeft aan dat dit een probleem is bij de implementatie van digitale transformaties. Een hoog percentage wanneer je bedenkt dat het overgrote gedeelte van de Nederlandse zorginstellingen al gebruikmaakt van veilige communicatie-oplossingen.

Veel organisaties zien door de complexiteit van de sector en wet- en regelgeving niet meer waar ze moeten beginnen en wat ze kunnen aanpakken. Daarnaast is zorg voor patiënten de eerste prioriteit. Digitale communicatie moet die ondersteunen en geen struikelblok zijn.

Zorginstellingen wachten daarom jaren op grote complexe programma's vanuit de overheid of grote consultancykantoren die uiteindelijk niet aan wensen voldoen. Deze programma's vragen veel energie en tijd. Dit staat digitalisering en innovatie behoorlijk in de weg. Dit whitepaper richt zich daarom op 8 uitdagingen op het gebied van digitale communicatie die organisaties vandaag al kunnen oplossen, een pragmatische aanpak.

We zien dat organisaties die digitale transformatie binnen communicatie succesvol weten te regelen zich vooral richten op wat ze vandaag wél kunnen doen: de mouwen opstropen en niet afwachten op de holy grail - die eigenlijk niet bestaat. Die Nederlandse mentaliteit heeft ons gebracht tot digitale voorloper in Europa.

Laten we het onszelf daarom niet moeilijker maken dan het eigenlijk is.

Inhoudsopgave

De volgende uitdagingen worden behandeld in dit whitepaper:

Leeswijzer

De uitdagingen in dit whitepaper zullen voor elke Security Professional in de zorg herkenbaar zijn en kunnen worden opgelost door de juiste implementatie van een veilig communicatieplatform. Bijna alle organisaties hebben anno 2020 een oplossing voor veilige digitale communicatie, maar lost je huidige leverancier deze cruciale uitdagingen op?

Daarom zijn de uitdagingen in dit whitepaper zo specifiek mogelijk gemaakt. Per uitdaging wordt uitgelegd hoe toonaangevende leveranciers voor veilige communicatie dit op kunnen lossen. Zo geeft dit whitepaper organisaties handvatten om deze uitdagingen op te lossen, processen te verbeteren en te heroverwegen of de huidige manier van werken de juiste is.

De tekst is op een praktische manier geschreven. De schrijver neemt je mee aan de hand van acht uitdagingen, de oplossingen, cruciale inzichten en voorbeelden uit de praktijk.

In het whitepaper worden praktijkvoorbeelden uit Nederland en België van de volgende organisaties uitgelicht: Universitair Ziekenhuis Antwerpen (UZA), St. Jans Gasthuis Weert (SJG Weert), Covid19 Sneltest, Buurtzorg, ChipSoft HiX, LIMOR, Centre Neuro Psychiatrique Saint-Martin en AT Osborne.

De schrijver neemt je mee aan de hand van:

1. de uitdaging;
2. belangrijke inzichten;
3. de oplossing;
4. praktijkvoorbeelden van zorginstellingen.

Uitdaging één

Risico verminderen op datalekken

Een datalek ontstaat als gevoelige persoonsgegevens beschikbaar zijn voor onbevoegden. De meeste mensen denken bij datalekken aan hackers die een slecht beveiligde database leegroven. In de praktijk blijken vooral menselijke fouten de oorzaak, fouten van medewerkers van de organisatie zelf. Ongelukjes en slordigheden die o.a. ontstaan door een hoge werkdruk waarbij zelden opzet in het spel is. Jaarlijks wordt zelfs meer dan 90% van de datalekken veroorzaakt door zo'n menselijke fout, zo blijkt uit onderzoeksrapporten van de **Autoriteit Persoonsgegevens.**

Een ongeluk zit dus in een klein hoekje. De gevolgen kunnen echter aanzienlijk zijn. Een datalek resulteert in veel gevallen in imagoschade, soms zelfs in een hoge boete, maar het grootste kostenplaatje hangt aan het oplossen van de schade. De hoge prijs die organisaties betalen voor een datalek ligt niet zozeer bij de (potentiële) boete, zoals veel mensen denken. Patiënten moeten erop vertrouwen dat hun gegevens veilig zijn bij de zorgverlener. Uit onderzoek van **IBM** blijkt dat de gemiddelde kosten van een datalek in de zorg rond de 6 miljoen liggen.

Het is niet voor niets dat deze uitdaging als eerste aan bod komt in dit whitepaper. Een investering in bewustwording voor medewerkers (via training, maar vooral via software) om veilig met deze informatie om te gaan verdient zichzelf gegarandeerd terug.

Inzicht

Datalekken voorkomen gaan hand-in-hand met het voorkomen van menselijke fouten. Alleen software-oplossingen die focussen op het voorkomen van die menselijke fouten, zullen echt bijdragen aan het verkleinen van het risico op datalekken. Uiteindelijk is gebruiksvriendelijkheid van die oplossing de doorslaggevende factor. Het blijven de mensen die achter de knoppen zitten.

De oplossing

Het oplossen van menselijke fouten klinkt als een moeilijke opgave - en dat is het ook. De menselijke fouten die datalekken veroorzaken zijn immers fouten die mensen vaak onbewust maken. De oplossing ligt daarom bij dit menselijke aspect: medewerkers helpen om op het juiste moment de juiste beveiliging toe te voegen aan hun communicatie (bijvoorbeeld middels slimme veilige communicatie software). Dit klinkt als een uitdaging die niet van vandaag op morgen opgelost is, maar niets is minder waar.

Enerzijds is het oplossen van deze uitdaging dus een stuk bewustwording dat je moet creëren bij medewerkers. In de meeste gevallen versleutelt een laptop automatisch alle opgeslagen data, maar als de laptoptas een blocnote met persoonsgegevens bevat, is er nog steeds sprake van een lek. Als je per ongeluk een verkeerde ontvanger informatie stuurt die niet voor hem of haar bedoeld was, is er eveneens sprake van een datalek. Daarom is de oplossing ook tweeledig.

Het tweede deel van de oplossing is gerelateerd aan software. Het is verstandig om software in te zetten die medewerkers actief assisteert bij het maken van de juiste keuzes. Het risico dat een verkeerde ontvanger inzage krijgt in gevoelige persoonsgegevens wordt geminimaliseerd als de gebruiker vooraf al de juiste ontvanger kiest en vervolgens de informatie versleuteld verstuurt.

Nu hoor ik je denken: “Wij hebben al software voor veilig e-mailen”. Veel organisaties hebben met de komst van de AVG destijds een keuze gemaakt voor dergelijke software, maar in de tussentijd is er veel veranderd. Er zitten veel verschillen tussen de diverse oplossingen op de markt. Daarom is het goed om na te denken welke uitdagingen echt opgelost worden met de huidige leverancier. Past de gekozen oplossing nog bij de specifieke uitdagingen van de zorgorganisatie anno 2020 en wat doet de oplossing specifiek om datalekken te voorkomen? Alleen als de software de gebruiker niet in de weg zit en de werkzaamheden niet onnodig complex maakt, levert het daadwerkelijk een bijdrage aan een veilige werkomgeving.

Software moet helpen waar het nodig is, maar je met rust laten als het niet nodig is. Als medewerkers echter extra handelingen moeten verrichten, zoals het handmatig versleutelen van bestanden, ervaren zij beveiliging als een last. Hierdoor zijn medewerkers eerder geneigd deze maatregelen te ontduiken en naar alternatieven te zoeken. Bij het evalueren van een oplossing is het daarom belangrijk om gebruiksvriendelijkheid centraal te stellen. Daarnaast zou een softwareleverancier ook moeten helpen om de bewustwording onder medewerkers te vergroten. Daarover meer in uitdaging 8; medewerkers zijn zich niet bewust dat privacygevoelige informatie veilig gedeeld moet worden.

Software moet helpen waar het nodig is, maar je met rust laten als het niet nodig is.

Praktijkvoorbeeld

Reinhart Maertens, CIO bij Universitair Ziekenhuis Antwerpen (UZA): “De gegevensdeling tussen de zorgverleners onderling was nog maar beperkt gecentraliseerd en beveiligd. Daarom werden nog heel wat documenten met gevoelige data via onbeveiligde kanalen doorgegeven naar andere zorgverleners. Willen we datalekken vermijden, dan dient dit op een beveiligde en gecontroleerde manier te gebeuren.”

Maertens vervolgt: “Het is goed om te benadrukken dat het inderdaad niet alleen gaat om medische gegevens maar ook administratieve gegevens die gevoelige data bevatten zoals financiële gegevens, persoonsgegevens, ga zo maar door. Dit wil ons ziekenhuis koste wat het kost ook beveiligd en gecontroleerd delen.”

Om het gevaar van datalekken te voorkomen implementeerde UZA software die gebruiksvriendelijkheid als uitgangspunt heeft. “Zivver is sterk geïntegreerd in Microsoft Outlook en Outlook is op haar beurt een zeer goed geadopteerde tool bij de UZA-medewerkers. Dat betekent dat het gebruik van Zivver snel en intuïtief opgezet kon worden”, aldus Reinhart. Omdat de aard van het systeem ook nog eens erg gebruiksvriendelijk is, zal dit op de langere termijn een positief effect hebben op de digitalisering van onze organisatie. Dat is erg belangrijk.”

Naast gebruiksvriendelijkheid is ook bewustwording een belangrijke factor om data “Zivver draagt bij aan de bewustwording van medewerkers doordat de technologie niet alleen waarschuwingen geeft tijdens het opstellen van een e-mail, maar echt de relatie analyseert tussen informatie, ontvanger én eerdere gedragspatronen. Zo zijn de waarschuwingen zoals “Weet je zeker dat je deze informatie onbeveiligd wil versturen, het bevat persoonsgegevens” relevant en niet spammerig.”

Organisatie

Universitair Ziekenhuis Antwerpen (UZA)

Medewerkers

+ 3.000

“Zivver is sterk geïntegreerd in Microsoft Outlook en Outlook is op haar beurt een zeer goed geadopteerde tool bij de UZA-medewerkers. Dat betekent dat het gebruik van Zivver snel en intuïtief opgezet kon worden”

Reinhart Maertens, CIO bij Universitair Ziekenhuis Antwerpen (UZA)

Uitdaging **twee**

Veilig communiceren met derde partijen ongeacht hun communicatie-oplossing en infrastructuur

Veilig communiceren moet gemakkelijk zijn, zowel intern als extern. Hier zitten echter nogal wat haken en ogen aan. Dit komt onder andere omdat het volgens wet- en regelgeving belangrijk is om inzicht te krijgen in wie wanneer toegang heeft tot welke privacygevoelige (medische) gegevens. Waarom is dat eigenlijk vastgelegd - en waarom is 'gewone' e-mail dan bijvoorbeeld niet veilig genoeg? En zijn post en de fax (nog verrassend veel gebruikt door zorgorganisaties) bijvoorbeeld wel veilig?

E-mail is nog steeds de meest gebruikte communicatievorm, ook in de zorgsector. Medewerkers spenderen gemiddeld twee uur per dag aan het werken met e-mail. Het mooie van e-mail is dat vrijwel iedereen het snapt, toegang tot e-mail heeft en dat er standaarden voor zijn. Het gaat om verschillende standaarden die in de loop der tijd zijn uitgebreid of aangevuld, waaronder SMTP, en STARTTLS.

Het nadeel van deze standaarden is echter dat ze, mede doordat ze stammen uit een tijd waarin veiligheid nog niet top of mind was, onvoldoende in staat zijn om de veiligheid te bieden die nodig is voor het uitwisselen van gevoelige (gezondheids) informatie. Deze standaarden hebben dan ook veel zwakke plekken en bovenal is STARTTLS bijvoorbeeld een opportunistisch protocol. Waarom? We duiken dieper de materie in. Ook al kan je tegenwoordig TLS met één klik inschakelen, het lost het probleem rondom veilig digitaal communiceren

Lees verder op de volgende pagina →

Inzicht

Zorginstellingen maken nog veelvuldig gebruik van fax en post omdat zij zich zorgen maken om de veiligheid en het gemak van digitaal communiceren. Dit staat digitalisering in de weg.

niet op. Je bent nog steeds afhankelijk van de serverinstellingen van de ontvanger. Om een veilige verbinding te maken, moeten zowel de verzender als de ontvanger TLS gebruiken. Wanneer er geen beveiligde verbinding kan worden gemaakt bij de ontvanger, levert Gmail bijvoorbeeld e-mails en bijlagen af via niet-beveiligde verbindingen - of helemaal niet.

Om deze tekortkomingen van e-mail te compenseren zijn leveranciers oplossingen gaan maken die wel de benodigde veiligheid bieden. Elke leverancier heeft echter zijn eigen oplossing bedacht, waardoor er inmiddels een aanzienlijk aantal losse oplossingen bestaan die niet met elkaar praten. Met als gevolg dat ontvangers last hebben van het feit dat de verzender een andere oplossing heeft gekozen dan zij en meestal moeten inloggen op een, vaak onhandig, portaal van een ander product. Wat niet alleen onhandig is, maar ook inefficiënt en communiceren niet vergemakkelijkt.

Om dit te verhelpen waren bindende afspraken over zogenaamde interoperabiliteit nodig. Een voorbeeld ter duiding: interoperabiliteit zorgt ervoor dat de consument X met zijn KPN-abonnement gewoon kan bellen met consument Y wanneer zij belt via het netwerk van VodafoneZiggo. De netwerken communiceren met elkaar zonder dat de consument het door heeft. Dit moet ook het geval zijn in het proces van beveiligde communicatie. Meer over interoperabiliteit bij ‘Uitdaging 7: Voldoen aan de NTA 7516 normering’.

De oplossing

Om deze - en andere uitdagingen - op te lossen werkten belanghebbenden en experts uit de zorg aan een normenkader voor veilige e-mail, waarin ook deze interoperabiliteit een belangrijke rol speelt. Het traject startte op 10 oktober 2018 en eindigde met de publicatie van de norm NTA 7516 in het voorjaar van 2019. Op 20 mei 2020 werd ook certificatie voor NTA 7516 mogelijk met de publicatie van het certificatieschema NCS 7516. Zowel zorgorganisaties als softwareleveranciers hebben zich te houden aan de norm. Dit zou het in de toekomst makkelijker moeten maken voor zorgorganisaties om hun communicatiestromen te digitaliseren en zo te innoveren.

De NTA 7516 legt de verantwoordelijkheid bij de verzender (zorgorganisatie) om te zorgen dat informatie veilig en geauthentiseerd bij de ontvanger terechtkomt. Deze verantwoordelijkheid van de verzender vloeit voort uit de AVG en specifieke aanwijzingen van de AP rondom toegangsbewaking. Vanuit het oogpunt van interoperabiliteit is het echter wenselijk en noodzakelijk om het mogelijk te maken deze verantwoordelijkheid over te dragen aan een ontvanger die zelf ook voldoet aan de NTA 7516. Door te voldoen aan de NTA 7516 geeft deze organisatie de garantie dat zij zelf zorg draagt voor passende beveiliging van berichten en authenticatie van gebruikers binnen haar eigen omgeving.
Er zitten echter wel haken en ogen aan de norm. Interoperabiliteit is de rode draad in de norm,

Leveranciers kunnen namelijk gecertificeerd zijn op verschillende punten binnen de NTA 7516-normering.

maar de norm bestaat uit veel meer dan dat. De norm beschrijft aan welke ruim twintig eisen organisaties en de oplossingen die zij gebruiken moeten voldoen als ze willen claimen veilig te zijn. Dit zijn eisen ten aanzien van beschikbaarheid, integriteit, vertrouwelijkheid, gebruiksvriendelijkheid, interoperabiliteit, beleid en logging. Leveranciers kunnen namelijk gecertificeerd zijn op verschillende punten binnen de NTA 7516-normering.

Om echt makkelijk met derden veilig te communiceren is dus noodzakelijk om een leverancier te kiezen die met alle systemen kan praten. Het niet hoeven aanmaken van een account om informatie te kunnen lezen en ontvangen is een van de punten uit de NTA 7516, maar dat is cruciaal om deze uitdaging op te lossen.

Advies is dus: voor het kiezen van een leverancier voor veilige communicatie is het cruciaal om op te vragen op welke punten zij NTA 7516 gecertificeerd zijn. Ga dan goed na welke punten voor jouw organisatie belangrijk zijn om het digitale communicatieproces zo gemakkelijk mogelijk te maken - en het allerbelangrijkste: stel interoperabiliteit centraal. Hierover meer in uitdaging 6; voldoen aan de NTA 7516 normering.

Praktijkvoorbeeld

“Voor de uitwisseling van patiëntgegevens met onze partners hebben we verschillende mogelijkheden”, vertelt Annemiek Knipscheer, voormalig Information Security Officer (ISO) van SJG Weert (tegenwoordig Information Security Officer (ISO) bij Catharina Ziekenhuis). “Via ons ziekenhuisinformatiesysteem en Zorgmail konden we bijvoorbeeld veilig informatie met huisartsen delen. Er was echter geen structurele oplossing voor veilige communicatie met partners waar wij zelf patiënten naar doorverwijzen. Fax bleek destijds dan het meest veilige middel. Maar dat is natuurlijk niet werkbaar. Om een structureel veiligere en meer gebruiksvriendelijke optie te kunnen bieden, kozen we voor een nieuwe - digitale - oplossing.”

Een ander belangrijk pluspunt is volgens Knipscheer het feit dat partners niet over een account hoeven te beschikken om informatie uit te wisselen. “Het doorverwijzen naar deze partners gebeurt ad hoc”, motiveert ze. “Het is praktisch onhaalbaar met al deze verschillende partijen aparte gebruiksafspraken te maken. Desalniettemin dwingen we onze partners met de introductie van een veilig kanaal tot een extra handeling. Onervaren gebruikers kunnen dit als complex ervaren. Mede daarom is de grote gebruiksvriendelijkheid en interoperabiliteit een belangrijk voordeel en cruciaal in het keuzeproces naar de juiste oplossing.”

Organisatie

SJG Weert

Medewerkers

+ 650

Uitdaging **drie**

E-mails vanuit EPD's zijn onveilig en EPD's communiceren niet goed met elkaar

Het EPD is dé belangrijkste bron voor communicatie over bijvoorbeeld afspraken en onderzoeksuitslagen, noem maar op. Versturen van deze informatie via reguliere e-mail is niet toegestaan sinds de komst van de Europese privacywetgeving (AVG) en specifieke normenkaders voor de zorg. Denk bijvoorbeeld aan de norm voor veilige ad hoc communicatie van gezondheidsinformatie, de NTA 7516. Veel organisaties vallen daardoor terug op het sturen van brieven. Dit leidt tot hogere kosten, zorgen over veiligheid en vertraging van communicatie.

Inzicht

Terugvallen op fax, post of koeriers voelt alsof organisaties stappen terug in de tijd zetten. Als 97% van de Nederlandse zorginstellingen werkt met een EPD, moet dit EPD ook veilig kunnen communiceren. De meeste EPD's hebben tegenwoordig integraties met andere oplossingen die het mogelijk maken om veilig (geautomatiseerd) te communiceren vanuit een EPD.

De oplossing

Door een koppeling van veilige communicatie oplossingen met EPD's hebben zorgorganisaties de mogelijkheid om bijvoorbeeld rechtstreeks afspraakbevestigingen te versturen naar het persoonlijke e-mailadres van de patiënt. Zivver realiseerde in samenwerking met verschillende ziekenhuizen koppelingen die veilig e-mailen vanuit hun EPD's mogelijk maken.

Met de Mail Submission module van Zivver kan zorginformatie rechtstreeks vanuit het bronsysteem (bijvoorbeeld ChipSoft HiX) veilig worden gemaild. Daarbij kunnen alle vertrouwde beveiligingsmaatregelen van Zivver worden toegepast, zoals twee-factor-authenticatie via SMS (eIDAS substantieel, verplicht onder de NTA 7516) en het instellen van een bepaalde beschikbaarheidstermijn voor het bericht. Snel, safe, simpel en met grote kostenbesparingen tot gevolg!

Praktijkvoorbeeld

Om berichten vanuit HiX veilig te versturen, gebruiken klanten van Zivver de Mail Submission-functionaliteit. Hiermee kan een applicatie of mailserver berichten aanbieden bij smtp.zivver.com. Voor het geautomatiseerd versturen van een veilig bericht direct vanuit ChipSoft HiX, wordt er een SMTP-systeemkoppeling opgezet met Zivver. HiX biedt het te versturen bericht aan de Zivver SMTP-server aan. Zivver verstuurt dit bericht vervolgens niet als 'normale' e-mail. De Zivver SMTP-server heeft een koppeling met de Zivver-server. Deze zorgt ervoor dat het aangeboden bericht als een Zivver-bericht wordt verstuurd, zodat het veilig bij de beoogde ontvangers wordt afgeleverd.

Organisatie

ChipSoft HiX

"Naast ChipSoft HiX integreert Zivver onder andere met JDS WIND!, Oase Dental, Evry, Exquise, Novadent en Simplex."

Rick Goud, CIO Zivver

Uitdaging **vier**

Testuitslagen en grote bestanden veilig delen

Met de uitbraak van het coronavirus is deze uitdaging relevanter dan ooit. Maar ook ver voor de uitbraak van het virus zochten testcentra, huisartsen en ziekenhuizen naar een oplossing om testuitslagen en grote bestanden snel te delen met betrokkenen en geautoriseerde behandelaren. Zowel bij een positieve, als een negatieve uitslag. In sommige gevallen wil je de patiënt direct op de hoogte brengen, maar in de meeste gevallen is het cruciaal dat de behandelende arts de uitslag van een onderzoek snel kan inzien. Moet je deze uitslag dan delen via fax of koerier? Organisaties die een oplossing hebben voor veilige e-mail kunnen deze uitslagen direct online delen.

Maar in bepaalde situaties zijn documenten met testuitslagen, onderzoeksstatistieken of bijvoorbeeld röntgenfoto's te groot om te delen als bijlage in een e-mail. Als gebruiker zit je al snel aan je limiet. Je kunt bijvoorbeeld met Gmail tot 25 MB aan bijlagen verzenden. Als je meerdere bestanden hebt, mogen ze gezamenlijk niet groter dan 25 MB zijn. In veel situaties worden testuitslagen en grote bestanden zoals foto's daarom verstuurd als CD-roms of zelfs floppies (welkom terug in de jaren '80!). Het zijn niet alleen testuitslagen die vaak op deze manier verstuurd worden. Als patiënten bijvoorbeeld van huisarts of ziekenhuis wisselen, worden dossiers nog steeds veel via post verstuurd van A naar B. Daarnaast hebben patienten en clienten recht op elektronische inzage en een elektronische kopie van hun medisch dossier. Deze kunnen zij te allen tijde opvragen. Het zou toch mooi zijn om die digitaal te kunnen versturen.

En dat kan al, begrijp ons niet verkeerd. Er zijn vele leveranciers op de markt voor het delen van grote bestanden zoals WeTransfer, DropSend en Smash. Alleen zijn deze vrijwel allemaal niet veilig genoeg voor het delen van privacygevoelige gegevens - en al helemaal niet geïntegreerd in e-mailclients zoals Outlook en Gmail. In vele gevallen moet je als gebruiker dus uit je 'normale' manier van werken om via een ander programma bijlagen - op een onveilige manier - te delen.

Inzicht

Als je voor grote bestanden alsnog terug moet vallen op platformen zoals WeTransfer, ondermijn je als het ware de inzet van je huidige veilige communicatie platform. WeTransfer en de meeste vergelijkbare tools kunnen namelijk de veiligheid van data niet garanderen en integreren niet in de huidige workflows.

De oplossing

Om deze informatieflows te digitaliseren moet gekeken worden naar integraties met systemen. Als je zelf deze informatie veilig wil versturen, kan dat natuurlijk al met sommige veilige e-mailleveranciers. Maar het is belangrijk dat leveranciers integraties hebben met huidige systemen zoals Gmail en Outlook en grote bijlagen kan versturen. Dan voorkom je dat gebruikers naar externe platformen gaan om grote bestanden veilig te delen. Waarom is dit belangrijk? Het is weer een extra handeling die mensen moeten doen. Elke extra handeling is een mogelijkheid voor de gebruiker om een afweging te maken om het toch onveilig te versturen. Bij een integratie van een dergelijk platform om grote bestanden te delen in je huidige e-mailclient is dat natuurlijk niet nodig.

Zivver integreert in Outlook en Gmail en dit maakt het mogelijk dat gebruikers bijlagen tot 5 TB beveiligd kunnen versturen vanuit hun eigen vertrouwde e-mailomgeving. Ja dat is Terabyte, en dus 5.000 Gigabyte!

Praktijkvoorbeeld

Bij het aanmelden voor een sneltest moet het persoonlijke 06-nummer en e-mailadres van de geteste persoon ingevuld worden. Dit is essentieel voor het delen van de testuitslag. Bij aankomst op de testlocatie wordt ter controle aan de geteste persoon gevraagd of de door hen opgegeven persoonsgegevens kloppen.

Ashmini Mangroelal van het Covid19 sneltestteam vertelt: “Na het testen wordt de uitslag binnen één uur bekendgemaakt. Dit bekend maken gaat via beveiligd e-mail. Omdat wij hierbij te maken hebben met persoonsgevoelige gegevens en de AVG wet- en regelgeving is het van belang dat deze testuitslag versleuteld en uitsluitend met de geteste persoon gedeeld wordt.”

“De geteste personen ontvangen een e-mail van het Covid19 sneltestteam. Om deze te kunnen lezen moet een persoonlijke sms-code ingevuld worden. De geautoriseerde ontvanger vult de code in en krijgt zo toegang tot de e-mail met zijn of haar testuitslag. Doordat de uitslagen versleuteld verstuurd worden, zorgen wij ervoor dat we volgens de AVG-richtlijnen te werk gaan. Zo hebben de geteste personen snel beveiligde toegang tot hun medische uitslag. En snelheid is van belang bij een pandemie.”

“Naast het delen van de testuitslag melden wij ook elke dag de positief geteste mensen bij de GGD. Onze arts doet deze meldingen eens per dag. Om het bestand met het overzicht van de positief geteste mensen naar de arts te mailen wordt ook gebruik gemaakt van Zivver.”

Organisatie

Covid19 sneltest

Uitdaging **vijf**

Hoe maak ik het proces van authenticatie (zoals 2FA) zo gebruiksvriendelijk mogelijk?

Elke zorgmedewerker herkent het wel: je krijgt dagelijks e-mails binnen van verschillende zorgorganisaties via platformen voor beveiligde e-mail. Je moet de hele dag verificatiecodes invoeren, vele wachtwoorden gebruiken om data in te zien of e-mails te openen en inloggen op verschillende systemen. Dit komt omdat organisaties verschillende leveranciers gebruiken om privacygevoelige data te verwerken.

Stel dat jouw organisatie bijvoorbeeld werkt met een functionele inbox (team@, secretariaat@), dan is het vaak niet mogelijk om beveiligd te mailen zonder veel extra handelingen. Dat terwijl je wel al een oplossing hebt voor veilig e-mailen. Nu moet je op zoek naar een andere oplossing voor functionele inboxen. Dat is als het ware een pleister voor op de wond zoeken, in plaats van genezen. Waarschijnlijk wil je als medewerkers maar een keer inloggen in een omgeving die alle collega's gebruiken binnen de organisatie.Een oplossing zou je moeten helpen ongeacht jouw uitdaging zoals veilig bestanden delen, veilig mailen, compliancy of functionele inboxen.

In een ideale wereld zouden veilige communicatie systemen alle mogelijkheden onder één dak hebben. Hoewel we als sector digitaal voorloper zijn in Europa, leven we (helaas) nog niet in die ideale wereld.

Inzicht

Organisaties die het aantal softwareleveranciers limiteren, zorgen ervoor dat medewerkers minder ongemak ervaren bij het gebruik. Daag daarom leveranciers uit om de voor jouw organisaties cruciale functionaliteiten onder een dak te hebben. Vaak is er meer mogelijk dan je initieel denkt.

De oplossing

Om werknemers te helpen om zo min mogelijk extra handelingen uit te voeren bij het beveiligen van communicatie is het cruciaal om zoveel mogelijk functionaliteiten onder te brengen bij een leverancier. Met name de functionaliteiten die je dagelijks vaak gebruikt. Op welke functionaliteiten je moet letten verschilt natuurlijk per organisatie. Het beste is om deze lijst op te stellen met medewerkers die dagelijks gebruik maken van oplossingen voor veilige communicatie. Onderstaand drie oplossingen die veel terugkomen bij zorginstellingen:

Interoperabiliteit

Lees verder bij 'Uitdaging 6: Voldoen aan de NTA 7516'. Interoperabiliteit is namelijk een van de belangrijkste pijlers van de NTA 7516 norm.

Functionele inboxen

Maar hoe zit dat dan voor functionele inboxen? Deze worden veelvuldig gebruikt in de zorg. Functionele of gedeelde mailboxen (team@, secretariaat@) mogen volgens wet- en regelgeving alleen nog maar gebruikt worden indien gebruikers met hun persoonlijke account toegang kunnen krijgen tot deze functionele mailbox (bijv. via autorisaties zoals vastgelegd in de Active Directory). Op deze manier wordt er gelogd welke gebruiker op welk moment namens een functionele mailbox heeft gehandeld - en dus toegang heeft gehad tot gevoelige informatie.

Deze tot op de persoon herleidbare toegang tot gevoelige informatie is ook een eis die voortvloeit uit de NEN 7513 en daarmee NEN 7510. Helaas bieden de meeste softwareleveranciers nog geen functionaliteiten voor functionele inboxen om gebruikers te beheren, geen ondersteuning voor gedelegeerde of team-accounts en geen functionaliteiten om gebruikers te authenticeren.

Dit betekent dat als zorgorganisaties gebruik willen blijven maken van gedelegeerde of functionele e-mailboxen voor het versturen en/of ontvangen van gevoelige informatie, hiervoor aanvullende maatregelen getroffen moeten worden. Hierbij moet dan ook de volledige logging van deze authenticatie en aansluiting daarop bij het werkelijk verzonden en ontvangen bericht worden geregeld. Een alternatief is besluiten dat functionele mailboxen niet meer kunnen worden gebruikt. Maar kiezen voor een leverancier die dit wel mogelijk maakt, is een veel betere oplossing.

Gebruiksvriendelijkheid: maak gebruik van een adresboek

Grote zorgorganisaties mailen met veel verschillende externe partijen. Om het makkelijker te maken om een ontvangerscontrole in te stellen voor de hele organisatie, hebben een aantal leveranciers een adresboek voor ontvangerscontrole ontwikkeld. In het adresboek staat welke extra beveiligingsmethode hoort bij een ontvanger. Dit kan bijvoorbeeld een wachtwoord of een 06-nummer zijn. Als de organisatie of een collega deze gegevens heeft ingesteld, kan iedere medewerker hier gebruik van maken. Bijvoorbeeld: wil je dat jouw contact een veilig bericht ontvangt dat hij kan openen met een sms-code? Dan heb je zijn 06-nummer nodig. Hier hoef je hem echter niet om te vragen als dit nummer al in het adresboek voor ontvangerscontrole staat.

Zo kan elke zorgmedewerker hem dus direct een bericht sturen. Hetzelfde geldt voor een bericht met toegangscode: als jouw contact met code in het adresboek voor ontvangerscontrole staat, hoef je geen code met hem af te spreken. De hele organisatie kan hier gebruik van maken, maar zij kunnen gegevens zoals het telefoonnummer niet inzien.

Praktijkvoorbeeld

Werken met te veel leveranciers voor veilige digitale communicatie was voor Buurtzorg een behoorlijk hoofdpijndossier. “Omdat wij een landelijk werkende organisatie zijn met meer dan 14.000 werknemers, hadden we te maken met veel verschillende vormen en aanbieders van veilige mailsystemen, met allerlei werkwijzen, inlogmethodes, ga zo maar door. Dit werkt natuurlijk erg onhandig. Dit uitte zich in frustratie, werknemers waren extra tijd kwijt met het versturen van privacygevoelige informatie. En daarbij waren sommige systemen simpelweg te ingewikkeld en niet altijd veilig genoeg.”, stelt Danielle Gérard, projectleider bij Buurtzorg.

“We hebben gekozen voor één ‘universeel’ systeem voor al onze medewerkers en teams, waarmee gemaild kan worden naar alle adressen, ook buiten de organisatie. Onze medewerkers kennen Gmail. Het was voor ons in de keuze van een platform dan ook belangrijk om voor deze integratie te kiezen. We willen medewerkers die niet gewend zijn om veel met computers te werken niet opzadelen met een ingewikkelde software-oplossing.”

Gérard besluit: “We gebruiken nu Zivver voor Gmail. Zivver is gewoon een eenvoudig systeem. De signalerende functie die onze medewerkers alerts geeft is voor ons erg belangrijk en draagt bij aan bewustwording. Het grote voordeel van Zivver is dat de ontvanger van veilige berichten geen gebruiker van Zivver hoeft te zijn. Zo kunnen we ook makkelijk met organisaties buiten Buurtzorg communiceren - en de tijd die we overhouden besteden aan het verlenen van zorg.”

Organisatie

Buurtzorg

Medewerkers

+ 14.000

“We hebben gekozen voor één ‘universeel’ systeem voor al onze medewerkers en teams, waarmee gemaild kan worden naar alle adressen, ook buiten de organisatie.”

Danielle Gérard, Projectleider Buurtzorg

Uitdaging **zes**

Voldoen aan de NTA 7516

Veel communicatie in en rond de zorg vindt op gestructureerde wijze plaats (denk aan mechanismen en standaarden zoals Edifact, IHE-profielen, etc.). De voorspelbaarheid en structuur maakt het relatief gemakkelijk om de bescherming van deze communicatie goed te regelen. Naast deze gestructureerde communicatiestromen, vindt er echter ook ongestructureerd ad-hoc berichtenverkeer plaats. Denk hierbij aan e-mail en chatapplicaties. De onvoorspelbaarheid van deze communicatievormen maakt het lastiger om ze goed te beschermen.

Uitdagingen voor zorgorganisaties:
Omdat het niet praktisch is om (bijvoorbeeld) voorafgaand aan iedere e-mail losse afspraken te moeten maken over hoe deze beveiligd wordt, biedt de NTA 7516 de oplossing door het geven van alle relevante criteria voor veilige ad-hoc communicatie. Op deze manier biedt de NTA 7516 duidelijkheid aan organisaties, leveranciers en patiënten/cliënten met betrekking tot wat wel en wat niet veilig is als het gaat om ad-hoc berichtenverkeer. De NTA 7516 is opgesteld door de NEN in opdracht van VWS en het werkveld, en wordt door de Inspectie Gezondheidszorg en Jeugd en Autoriteit Persoonsgegevens gebruikt als toetsingskader.

De NTA 7516 beschrijft ca. 25 eisen waar organisaties zoals wij aan moeten voldoen. Een groot deel (circa 18) van de eisen is technisch van aard, een deel (circa 7) beleidsmatig. De eisen

Lees verder op de volgende pagina →

Inzicht

Waar een zorgorganisatie aan alle eisen moet voldoen, mag een leverancier zelf kiezen voor welke eisen hij zich laat certificeren en welke specifieke inspanning hij levert op die eis. Hierdoor ontstaat verwarring bij veel zorgorganisaties: de ene NTA 7516-certificering is dus de andere niet.

gaan onder andere over de beschikbaarheid, integriteit, vertrouwelijkheid, gebruiksvriendelijkheid, interoperabiliteit, beleid en logging rondom onze communicatie oplossingen. Deze eisen vloeien voor een deel voort uit de wet (met name de AVG) en voor een deel uit gebruikerswensen die door de NEN zijn geïnventariseerd.

Uitdagingen voor zorgorganisaties met betrekking tot leveranciers:
Naast het feit dat zorgorganisaties moeten voldoen aan de eisen van de NTA 7516, is het ook belangrijk dat leveranciers NTA 7516-gecertificeerd zijn. Een belangrijk aandachtspunt hier is dat leveranciers zelf mogen bepalen voor welke eisen zij zich laten certificeren en welke prestatie zij leveren op bepaalde criteria. Zo kan een leverancier er bijvoorbeeld voor kiezen om zich helemaal niet te laten certificeren op een bepaalde eis, bijv. toegangsvertrouwelijkheid, en voor een andere eis, zoals beschikbaarheid, slechts een bepaalde prestatie te garanderen (bijv. een beschikbaarheid van 98% in plaats van 100%).

Dit is een belangrijk punt aangezien het grote consequenties kan hebben voor de zorgorganisatie. Zoals gezegd is het namelijk de eigen verantwoordelijkheid om te voldoen aan alle eisen. Indien de gecertificeerde leverancier waar je als zorgorganisatie mee werkt slechts op een gedeelte van de eisen is gecertificeerd, moet er voor de overgebleven punten zelf geïnvesteerd worden. Dit komt vaak in de vorm van extra maatregelen of samenwerkingen met meerdere leveranciers om de gaten te dichten.

Een belangrijke eis van de NTA 7516 waar iedere leverancier wel aan moet voldoen, is de zogenaamde interoperabiliteit. Dit principe zorgt ervoor dat organisaties die aan de NTA 7516 voldoen gemakkelijk en veilig berichten uit kunnen wisselen met andere organisaties die aan de norm voldoen, ook al gebruiken beide een andere leverancier.

De eerste vraag is natuurlijk “Wat is interoperabiliteit?”. Interoperabiliteit is ‘de mogelijkheid van verschillende autonome, heterogene systemen, apparaten of andere eenheden (bijvoorbeeld organisaties of landen) om met elkaar te communiceren en samen te werken. Om dit te bewerkstelligen zijn standaarden, protocollen en procedures nodig voor de afstemming van de verschillende entiteiten op elkaar’.

Samengevat betekent interoperabiliteit dus met elkaar kunnen communiceren op basis van standaarden. Dus zonder standaarden geen interoperabiliteit. Zonder standaarden voor fittingen van lampen, hadden we geen ledlampen van verschillende leveranciers in onze lampen kunnen gebruiken. Zonder een standaard voor stopcontacten en stekkers, hadden we niet elk apparaat in elk willekeurig stopcontact kunnen steken. Hetzelfde geldt voor het feit dat we met elkaar kunnen bellen ongeacht waar we ons abonnement hebben afgesloten. KPN zorgt ervoor dat hij altijd kan communiceren met een andere lijn, ongeacht of dat VodafoneZiggo of Lebara is.

Vooralsnog is de NTA 7516 een Nederlandse norm, deze geldt dus niet voor België. De NEN heeft wel laten weten dat zij de intentie heeft om een traject te starten om deze norm tot een Europese CEN-norm te maken. Nederland is namelijk het eerste land dat een dergelijke norm voor veilige ad hoc communicatie heeft opgesteld. Vaak worden dit soort normen centraal of decentraal overgenomen door andere bij de CEN aangesloten landen, waaronder alle 28 Europese lidstaten.

De oplossing

Checken! Vraag bij je huidige oplossing op hoe de leverancier invulling heeft gegeven aan deze eisen. Het document 'Verklaringen voor in- en uitsluitingen' van de leverancier (bekijk hier een voorbeeld) en ook de technische handleiding zouden daar de juiste inzichten over moeten geven. Kies vervolgens voor een leverancier die aan zoveel mogelijk eisen voldoet en hulp aanbiedt bij de beleidsmatige eisen. Dan maak je het jezelf makkelijker en kan je sneller compliance realiseren.

Met Zivver weet je zeker dat je aan alle eisen die aan een leverancier worden gesteld voldoet. Daarnaast helpt Zivver je ook met eisen rondom het beleid door middel van templates en workshops. Zivver biedt een NTA 7516-consult waarmee organisaties kosteloos kunnen checken in hoeverre zij op het moment voldoen aan de norm.

Uiteindelijk zijn zorgorganisaties die voldoen aan de NTA 7516 normering interoperabel. Als er sprake is van interoperabiliteit, betekent dat gegarandeerd een vermindering van het aantal authenticaties op een dag. Zoals eerder beschreven zorgt het principe van interoperabiliteit ervoor dat organisaties - mits ze aan alle eisen van de NTA 7516 voldoen en werken met een gecertificeerde leverancier - makkelijk en veilig berichten uit kunnen wisselen met organisaties die ook interoperabel zijn. Het goede nieuws; volgens wet- en regelgeving zouden alle zorgorganisaties in 2020 al operabel moeten zijn.

Hoe werkt dat in de praktijk? Interoperabiliteit werkt als volgt: als Arts 1 (die werkt bij een zorginstelling die NTA 7516 gecertificeerd is) de analyse van zijn onderzoek met privacygevoelige medische gegevens beveiligd mailt naar Arts 2 (die tevens werkt bij een zorginstelling die voldoet aan de NTA 7516 norm), hoeft Arts 2 in dit geval geen extra authenticatie in te voeren om de informatie in te kunnen zien.

Hoe komt dat? Doordat de oplossing voor veilig e-mailen geïntegreerd is in zijn inbox en e-mail client of de gebruiker heeft ingelogd bij de web applicatie. Om in te loggen in zijn inbox (e-mailclient), heeft Arts 2 namelijk al zijn wachtwoord, en in veel gevallen specifieke authenticatie, ingevoerd. We weten nu dus zeker Arts 2 echt degene is, die hij zegt dat hij is. Bij het ontvangen van de analyse van Arts 1, hoeft hij dus geen wachtwoord, sms-code of andere authenticatie in te voeren. Dit heeft hij al gedaan toen hij inlogde bij zijn e-mailclient (of werkplek).

Samengevat betekent interoperabiliteit dus met elkaar kunnen communiceren op basis van standaarden. Dus zonder standaarden geen interoperabiliteit

Praktijkvoorbeeld

LIMOR is de Landelijke Instelling voor Maatschappelijke Ondersteuning en Rehabilitatie. De organisatie is er voor mensen die om welke reden dan ook diep in de problemen zijn geraakt en nergens anders terechtkunnen. Denk aan dak- en thuislozen, verslaafden, ex-gedetineerden, mensen met psychische problemen of schulden. LIMOR is dus geen zorgorganisatie, maar moet toch aan de NTA 7516 voldoen. Hoe zit dat precies? Dat is zo omdat de organisatie toch veel zorggerelateerde gegevens verwerkt. En dat geldt ook voor bijvoorbeeld gemeenten, overheidsinstellingen en andere communicatiepartners.

Organisatie

LIMOR

Medewerkers

+ 300

“De e-mails die wij beveiligd versturen via Zivver worden gewoon verzonden vanuit Outlook. Bij specifieke kernwoorden meldt Zivver dat beveiligd mailen de voorkeur heeft. Deze waarschuwing krijgen collega’s tijdens het opstellen van de mail, voordat ze hem versturen.
Omdat Zivver op deze manier integreert met Outlook, zijn er nooit grote wijzigingen voor gebruikers geweest.”

“Mede hierom hebben we de tool snel en gemakkelijk kunnen implementeren. Door de integratie met Outlook merk je eigenlijk niet dat Zivver aan staat. De tool is erg gebruiksvriendelijk, parameters zijn door organisatie zelf in te stellen, en ondertussen stimuleert Zivver verdere digitalisering van onze organisatie doordat we steeds meer data veilig online delen. Dat moet wel veilig, volgens wet- en regelgeving, en het is belangrijk controle over deze informatiedeling te houden”, aldus Mirella van Poelgeest Manager Bestuurssecretariaat, Communicatie & PR.

AT Osborne:
Maar ook bijvoorbeeld consultancypartners van zorginstellingen dienen veilig digitaal te communiceren. Op het eerste gezicht staat dit wellicht ver af van zorginstellingen. Maar ook zij verwerken privacygevoelige en soms medische informatie en dus vallen zij ook onder de NTA 7516-norm. “Het werkt twee kanten op”, stelt Elske Visser, Adviseur bij AT Osborne. Visser gebruikt Zivver operationeel vooral als ze met zorginstanties moet schakelen. “Als deze organisaties grote databestanden met ons willen delen, sturen we ze gewoon een Zivverbericht. Dan kunnen ze daarop antwoorden en beveiligd bestanden met ons delen tot 5.000 GB.”

Organisatie

AT Osborne

Medewerkers

+ 150

“Het is eigenlijk heel simpel,” stelt Mario Vermunt. “Voorheen werden veel gegevens via USB-stick of e-mail uitgewisseld. We vonden dat dit veiliger moest kunnen, wanneer nodig, want we moeten het niet onnodig complex gaan maken.”

Uitdaging **zeven**

Mijn medewerkers zijn zich niet bewust dat privacygevoelige informatie veilig gedeeld moet worden

Het is heel cliché, maar helaas nog altijd waar. De mens is de zwakste schakel in het beveiligen van data. De reden daarvoor is dat het beveiligen van data erom draait dat er geen gegevens worden verstuurd naar, of toegankelijk zijn voor, diegenen die geen toegang zouden moeten hebben tot die gegevens. Als dat een probleem is dat je wilt oplossen, moeten organisaties verder kijken dan alleen technische oplossingen. Het zijn immers mensen die die informatie delen.

Het komt vaak voor dat medewerkers niet precies weten wanneer ze bepaalde informatie beveiligd of onveilig kunnen versturen. En zelfs als ze het wel weten, komt het voor dat ze soms even niet opletten. Een gebruiksvriendelijke oplossing zorgt dat medewerkers eerder gebruikmaken van de software. Dit hebben we in ‘Uitdaging 1: datalekken voorkomen’ uitgebreid behandeld. Maar draagt dit ook bij aan de bewustwording? Zorgmedewerkers verwerken immers zoveel informatie op een dag, een foutje is snel gemaakt. Ook met gebruiksvriendelijke software.

Awareness campagnes zijn een stap in de goede richting, maar lossen dit niet geheel op. Naast zulke campagnes zou veilige communicatie software medewerkers moeten helpen betere beslissingen te nemen. Ze snappen wel dat informatiebeveiliging belangrijk is, maar hebben soms een geheugensteuntje nodig bij het toepassen van de juiste beveiliging. Wat namelijk altijd terugkomt (en terecht) is dat medewerkers zich vooral willen focussen op het menselijke aspect in de zorg.

Lees verder op de volgende pagina →

Inzicht

Veilige communicatiesoftware zou functionaliteiten moeten hebben die een bijdrage leveren aan de bewustwording van medewerkers.

Zorgmedewerkers komen ‘s ochtends hun bed uit om goede zorg leveren - en het beveiligen van data hoort daar volgens hen niet altijd bij. Maar als het verkeerd gaat, kan dit voor de patiënt vervelende gevolgen hebben. Een voorbeeld: de persoonsgegevens van patiënt1, gekoppeld aan bijvoorbeeld een GGZ-instelling, onthult een bijzonder gevoelige gezondheidskwestie. Het zou een grote ramp zijn voor de reputatie van medische organisaties als deze gegevens openbaar worden. En natuurlijk zijn de gevolgen voor patiënten niet te overzien.

Vaak beseffen zorgmedewerkers niet dat beveiliging juist uiteindelijk bijdraagt aan het leveren van goede zorg. Het is daarom cruciaal dat zij snappen en worden herinnerd aan wat het is dat ze moeten doen om veilig te communiceren. Als een relevante waarschuwing van een software-oplossing op de juiste momenten op-popt; “Let op; je verstuurt privacygevoelige informatie onveilig”, komt de handeling van beveiligd e-mailen vanzelf in het systeem van medewerkers.

De oplossing

It takes two to tango. De oplossing voor deze uitdaging is dus een mix van menselijke en technische factoren, die een synergetisch effect hebben op elkaar. Uiteindelijk zal de software de kans op een menselijke fout fors verkleinen. Maar het zijn alsnog de mensen die achter de knoppen zitten. Het advies is om daarom te kiezen voor een leverancier die gebruik maakt van relevante waarschuwingen die op het juiste moment helpen om het correcte beveiligingsniveau toe te passen.

Hoe werkt dat precies? De plugin van de veilige communicatiesoftware toetst bijvoorbeeld automatisch berichten en bijlagen op bepaalde regels en gevoelige inhoud - al tijdens het opstellen van je e-mail. De zorgorganisatie bepaalt zelf welke regels dit zijn. Deze zogenaamde ‘Bedrijfsregels’ laten de gebruiker nadenken of het bericht veilig moet worden verzonden, of niet. De Zivver-werkbalk geeft aan of er gevoelige inhoud is gevonden.

Tijdens het opstellen of verzenden van een bericht verschijnt er mogelijk een melding in de Zivver-werkbalk. Zoals bijvoorbeeld: Weet je zeker dat je “medische” informatie naar voorbeeld@email.com wilt versturen? Gebruikers kunnen op de melding klikken om te zien wat er aan de hand is.

Er zijn meerdere oplossingen op de markt die dit kunnen, maar wat voor veel zorgorganisaties de doorslaggevende factor is om voor Zivver te kiezen is de technologie die niet alleen een waarschuwing geeft, maar echt de relatie analyseert tussen informatie, ontvanger en eerdere gedragspatronen. Dit stelt Zivver in staat om de gebruiker te voorzien van contextspecifieke en relevante alerts, die effectief kunnen helpen bij het voorkomen van datalekken. Een voorbeeld hiervan is: je verstuurt gevoelige informatie naar iemand naar wie je nog nooit eerder gevoelige informatie hebt verstuurd. Maar nog belangrijker is de zorgverlener met rust te laten als alles goed gaat.

Praktijkvoorbeeld

“Wij zijn een ziekenhuis met één specialiteit, namelijk psychiatrische zorg. Onze experts behandelen een uiteenlopende patiëntenpopulatie; van depressies tot eetstoornissen en verslavingen, maar we bieden bijvoorbeeld ook forensische psychiatrie. De naam van de patiënt, gekoppeld aan onze instelling, onthult een bijzonder gevoelige gezondheidskwestie. Het zou een grote ramp zijn voor de reputatie van onze kliniek als deze gegevens openbaar worden. En natuurlijk zijn de gevolgen voor patiënten niet te overzien.”

De medewerkers van de kliniek e-mailen in Frans, Engels en Nederlands. Belgische organisaties hoeven niet te voldoen aan de NTA 7516-norm. Toch is bewustwording voor de organisatie een belangrijke pijler.

“De software van Zivver scant de e-mails en bijlagen in al deze talen tijdens het opstellen. Sectorspecifieke bedrijfsregels zorgen ervoor dat het juiste beveiligingsniveau voor elk bericht telkens wordt toegepast en eenvoudig kan worden aangepast als dat nodig is. Deze regels helpen om de controle over informatiebeveiliging te behouden en tegelijkertijd te voldoen aan de wettelijke vereisten. Zo worden medewerkers er dagelijks aan herinnerd hoe ze met privacygevoelige informatie moeten omgaan.”

Organisatie

Centre Neuro Psychiatrique Saint-Martin

Medewerkers

+ 100

“De software van Zivver scant de e-mails en bijlagen in al deze talen tijdens het opstellen. Sectorspecifieke bedrijfsregels zorgen ervoor dat het juiste beveiligingsniveau voor elk bericht telkens wordt toegepast en eenvoudig kan worden aangepast als dat nodig is.”

Pierre Wautier, CISO (Conseiller en sécurité de l’information)

Uitdaging **acht**

Patiënten en partners weten niet hoe ze zelf veilig contact met de zorgorganisatie op kunnen nemen

Als medewerker van een organisatie deel je veel gevoelige informatie met vaste (keten)partners. Denk aan zorgverleners, leveranciers en overheden. Zelf doe je dit veilig via een software-oplossing voor veilige communicatie.

Maar externen, patiënten en cliënten zonder veilige communicatie-oplossing hebben geen manier om makkelijk en veilig contact met jouw organisatie op te nemen. Zelf een veilige mail naar de ontvanger sturen zodat zij daarop veilig reageren is niet praktisch en al helemaal niet efficiënt. Stel dat cliënten contact opnemen (en daarbij gevoelige informatie delen) via een contactformulier op de website. Dan wordt deze informatie alsnog onbeveiligd gedeeld en komt de informatie binnen in een onbeveiligde omgeving. In veel gevallen een functionele inbox.
De zorgorganisatie zelf zal echter vaak informatie uitwisselen met vaste contacten zoals ketenpartners, leveranciers en klanten of cliënten. Voor efficiëntie in de samenwerking kan deze relatie snel en direct (privacy)gevoelige informatie of documenten aan de organisatie leveren. Denk bijvoorbeeld aan het doorverwijzen van een patiënt naar een zorginstelling, het aanleveren van financiële documenten of het versturen van contracten. In deze gevallen is het handig als de persoon die deze informatie verwerkt de documenten direct in zijn of haar inbox ontvangt.

Inzicht

Als je als organisatie alles goed hebt ingeregeld, dan is het fijn als je diezelfde mogelijkheid kan bieden voor patiënten. Liefst wil je natuurlijk niet dat zij een paspoort of medische gegevens delen via een onveilig contactformulier. Dan komen deze gegevens alsnog onveilig binnen - en vormen daarmee een gevaar.

De oplossing

Een aantal softwareleveranciers hebben daarom een zogenaamde Conversatiestarter. Dat werkt als volgt: met een Mail mij veilig-knop (of een andere conversatiestarter) op de website bied je externen een manier om verantwoord privacygevoelige informatie en documenten aan te leveren. In veel gevallen wordt deze conversatiestarter ook aangeboden op dezelfde pagina als het contactformulier.

Het bericht komt centraal binnen op het door jou ingestelde e-mailadres. Dit kan een functionele inbox of een persoonlijke inbox zijn. Op deze manier wordt de informatie ook snel verwerkt en wordt het niet onnodig moeilijk gemaakt om veilig te communiceren. Zo kan iedereen veilig contact opnemen via deze conversatiestarter op de website zonder dat ze een account hoeven aan te maken. Zelfs die patiënten en cliënten die dit 'spontaan' willen doen.

Daarnaast worden conversatiestarters bijvoorbeeld gebruikt als link in e-mailhandtekeningen. Zo faciliteer je relaties waarmee je veel communiceert om makkelijk en veilig met jou te mailen.

Voorbeeld: "PS: Graag wijs ik u op de link hieronder. Via deze link kunt u mij in het vervolg op eenvoudige wijze mails en documenten toezenden. Zo kunnen wij de privacy van de cliënten waarborgen. Mail mij veilig"

Voorbeeld uit de praktijk

Medlon is het laboratorium dat medische diagnostiek levert van bloedafname tot uitslag voor patiënten van huisartsen, specialisten en organisaties als Arbodiensten. Daarbij communiceert de organisatie met vele organisaties en partners. Om te voorkomen dat partners op een onveilige manier contact opnemen en persoonsgegevens delen, voegde zij de conversatiestarter toe aan de contactpagina. De volgende boodschap is zichtbaar op de contactpagina:

"Medlon gebruikt Zivver voor veilig mailen en bestanden delen. Niet-privacygevoelige informatie kan zonder gebruik van Zivver worden gedeeld. Wilt u echter privacygevoelige informatie naar ons mailen en heeft u geen Zivver? Via deze link kunt u zonder Zivver op een veilige manier een e-mail sturen naar iemand bij Medlon."

Organisatie

Medlon

Medewerkers

+ 175

Bedankt voor het lezen!

We hopen dat dit whitepaper handvatten biedt om uitdagingen rondom digitale communicatie op een praktische manier op te lossen. Mocht je in contact willen komen met organisaties uit de voorbeelden in het whitepaper, laat het ons dan weten. Samen kunnen we de digitale wereld een stukje veiliger maken.

Met Zivver kunnen zorginstellingen privacygevoelige informatie op een digitale manier, conform de AVG en NTA 7516, delen met patiënten, collega's en externe partijen.

Benieuwd wat Zivver voor jouw organisatie kan betekenen, of hoe Zivver anders is dan je huidige leverancier? Neem dan gerust contact op via **contact@zivver.com.**

Zivver B.V
Kon. Wilhelminaplein 30
1062 KR Amsterdam

085 016 0555
contact@zivver.com

www.zivver.com

linkedin.com/company/zivver facebook.com/zivver @zivver_nl