Help, ik mag niet meer e-mailen!

Vanaf mei 2018 is beveiligde e-mail de enige manier om persoonlijke gegevens te versturen. Secumail biedt hiervoor de oplossing aan.

Wat is het resultaat met Secumail?

Je e-mail wordt gegarandeerd veilig bezorgd met end-to-end versleutelde verbindingen, zonder dat de ontvanger daar iets voor hoeft te doen. Als verzender hoef je geen software te installeren. Integratie met Secumail kan op basis van een standaard e-mail koppeling of door gebruik te maken van de Secumail Web API.

Secumail doet het anders. Onze aanpak lijkt op wat je als consument ervaart als je gaat internetbankieren, gaat webshoppen of online je tickets koopt. Laagdrempelig, veilig en zonder gedoe.

Datalekken en de wet

De GDPR is in mei 2016 in werking getreden. Van organisaties wordt verwacht dat zij vanaf die tijd hun bedrijfsvoering met de GDPR in overeenstemming brengen. Zij krijgen daarvoor tot 25 mei 2018 de tijd. Daarna mag iedereen organisaties op de naleving van de GDPR aanspreken. De maximale boete is 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet in het geval van een onderneming, afhankelijk van welk bedrag hoger is.

General Data Protection Regulation (GDPR) Op 25 mei 2018 wordt de "General Data Protection Regulation" (GDPR) Verordening van kracht binnen de Europese Unie. Bedrijven en organisaties in heel Nederland mogen vanaf dan alleen onder strikte voorwaarden persoonlijke informatie verwerken. Houd je je er niet aan? Dan ben je strafbaar. De nieuwe richtlijn heeft veel impact op bedrijven en organisaties die persoonlijke informatie versturen via e-mail.

Datalekken De aanleiding voor de GDPR Verordening is onder andere het voorkomen van datalekken. Wat zijn datalekken?
Technisch is het mogelijk dat een e-mail (zonder toestemming van de rechter) wordt onderschept door criminelen of zelfs een (buitenlandse) overheid. Ook is het mogelijk dat de e-mail wordt verstuurd naar het verkeerde adres. Als dit een bestaand adres is, kan iemand anders de e-mail lezen.
Tot slot is het mogelijk om de inhoud van de e-mail te wijzigen, zonder dat de verzender en/of ontvanger dit weet. Uit onderzoek blijkt dat 47% van alle onbedoelde data lekken wordt veroorzaakt door email [bron: InfoWatch].

Wat moet ik doen volgens de wet? In de wet staat dat je "passende technische en organisatorische beveiligingsmaatregelen" moet nemen. We leggen in deze whitepaper uit wat praktisch haalbaar is om te voldoen aan de wet.

Privacy by Design wordt verplicht. Waar gebruikers hun privacy instellingen zelf kunnen aanpassen moeten deze instellingen als standaard op het hoogste niveau worden ingesteld.

E-mailen is niet veilig

Waarom is e-mailen eigenlijk niet veilig? Bij het versturen en ontvangen van e-mail zijn meerdere partijen betrokken: de mailserver of internet service provider van de verzender, de mailserver of internet service provider van de ontvanger en eventuele anti-spam en antivirus partijen. Van de meeste van deze partijen heb je hoogstwaarschijnlijk geen weet hoe ze hun beveiliging hebben ingericht.

Wat is beveiligde e-mail?

Beveiligde e-mail is een verzamelnaam voor verschillende methoden en technieken om e-mail berichten te beschermen tegen ongewenste inzage of ongewenste veranderingen.

Waarom is beveiligde e-mail belangrijk?

Bedrijven en organisaties die persoonsgegevens en bijzondere persoonsgegevens versturen via e-mail moeten maatregelen treffen waardoor die gegevens beschermd zijn tegen ongewenste inzage of ongewenste veranderingen. Normale e-mail is onvoldoende beschermd tegen ongewenste inzage of ongewenste veranderingen en voldoet daarmee dus niet aan de GDPR.

Geen garanties

Er is geen enkele garantie af te geven dat alle stappen in het e-mailproces met veilige verbindingen hebben plaatsgevonden. Sommige mailservers versleutelen het transport, andere mailservers doen dat niet. Daarnaast kan de ontvangende partij de e-mail na ontvangst wijzigen waardoor je als verzender met lege handen staat. Je kunt niet aantonen dat de inhoud is gewijzigd.

E-mail is een open systeem, zonder controle van de identiteit van de verzender. Hierdoor kunnen verzenders zich anders voordoen en denk je dat je een veilige e-mail krijgt, maar is dat niet zo. Hierdoor kunnen er vervelende extra zaken bij een e-mail zitten zoals virussen of spam.

Er is geen andere partij in de Nederlandse markt die een vergelijkbaar niveau van e-mail beveiliging en gebruiksgemak biedt.

Oplossingen zijn óf vreselijk complex óf het is geen echte e-mail

De kern van het beveiligde e-mail probleem

Vanaf 25 mei 2018 is het verplicht om gebruik te maken van een beveiligde e-mail oplossing wanneer een bedrijf of organisatie persoonlijke informatie communiceert via e-mail. De bestaande oplossingen zijn niet goed bruikbaar voor inzet bij burgers, consumenten of patiënten. Ze zijn óf vreselijk complex óf het is geen echte e-mail.

Wat is er mis met beveiligde e-mail? Er zijn diverse beveiligde e-mail oplossingen in omloop. De klassieke oplossingen vallen uiteen in twee benaderingen, waarbij de eerste benadering het bericht zelf versleutelt, dit wordt ook wel encryptie genoemd. De tweede benadering is een beveiligde web omgeving (“Mijn omgeving”) waarop ingelogd moet worden. Beide benaderingen hebben grote nadelen, ze zijn óf veel te complex óf het is te veel gedoe en mensen willen het niet gebruiken.

Waarom berichtversleuteling in de praktijk niet werkt

Het is veel te complex. Zelfs IT-specialisten vinden het een moeilijk onderwerp. Om veilig met elkaar te kunnen communiceren hebben zowel verzender als ontvanger een cryptografische sleutelset nodig. Vanuit het perspectief van een bedrijf of organisatie betekent dit dat je voor alle ontvangers een sleutelset moet laten genereren, voor elk apparaat dat de ontvanger heeft. Dat genereren en installeren van een sleutelset moet vervolgens ook nog eens gedaan worden door de ontvanger zelf. Dat is waar het spaak loopt. Het vraagt veel kennis en inzet van de ontvangende partij. Als die partij een burger, consument of patiënt is, zal duidelijk zijn dat dit te veel gevraagd is en in de praktijk niet gaat werken.

Waarom de web portaal oplossing in de praktijk niet werkt

Bij een web portaal oplossing krijgt de ontvanger een link toe gemaild via e-mail. Door op de link te klikken wordt er een web portaal geopend. Hierin is de e-mail te zien. Het bezwaar van deze manier van werken is dat de ontvanger niet de e-mail direct ontvangt in zijn/haar inbox, maar gedwongen wordt om de browser te openen en naar een website toe gaan. Weinig ontvangers nemen deze moeite, zoals blijkt uit recente issues die zijn ontstaan doordat burgers niet inloggen op het “Mijn Overheid” portaal. De ontvanger ervaart “portaalmoeheid”, van alle kanten wordt hij/zij belaagd met portalen, met eigen accounts, met als resultaat dat er niet ingelogd wordt en de ontvanger wacht totdat er een brief wordt gestuurd.
Daar komt tevens bij dat er vanuit de banken veel gewaarschuwd wordt voor het klikken op links in e-mail in verband met phishing aanvallen. Het concept van web portalen voor beveiligde e-mail staat daarmee sterk onder druk.

De Secumail oplossing

Wij doen het anders dan de oude oplossingen! We vragen niet aan ontvangers om te gaan werken met cryptografische sleutels en we vallen ze niet lastig met web portalen. Kies voor Secumail. Secumail biedt een pure e-mail ervaring en stelt geen eisen aan de ontvanger. Toch is de oplossing veilig en voldoet ze aan de GDPR.

Bewerkersovereenkomst

Secumail bewaart geen gegevens anders dan de meta data van de verzonden e-mails. Dit is te vergelijken met de enveloppe van een brief. In tegenstelling tot een brief bevat de meta-data van een e-mail ook het onderwerp zoals de verzender die opgeeft. In sommige gevallen kan hieruit vertrouwelijke informatie afgeleid worden. Daarom adviseert Secumail om een bewerkersovereenkomst op te stellen met iedere klant.

Veilig platform

Secumail biedt haar dienstverlening aan als een platform. Al het werk zit aan onze kant, zodat je als verzender geen moeilijke integraties hebt en als ontvanger niet geconfronteerd wordt met complexe technologie.

Andere aanpak

Secumail kiest voor een andere benadering. Onze aanpak lijkt op wat je als consument ervaart als je gaat internetbankieren, gaat webshoppen of online je tickets koopt. Bij internetbankieren merk je bijvoorbeeld heel weinig van de beveiliging die banken gebruiken om ervoor te zorgen dat niemand anders bij je bankgegevens kan komen. Toch gebeurt er een hoop onder de motorkap.

De bank zorgt voor een versleutelde verbinding met je browser of je telefoon en er wordt gecontroleerd of niemand meeluistert. Je zult moeten inloggen om aan te tonen dat je toegang hebt tot de informatie.

Deze aanpak is succesvol. Consumenten gebruiken inmiddels al jaren internetbankieren, kopen bij webshops en boeken online tickets. Het is zeer veilig gebleken en het heeft geleid tot een enorme stijging van het gebruik van online diensten.

Het Secumail geheim

Het geheim van Secumail is dat we gebruik maken van dezelfde technologie als bij online kanalen en die technieken optimaliseren voor e-mail.

Als verzender maak je bij Secumail deel uit van een gesloten netwerk, waarbij we je identiteit vaststellen voordat je e-mail kunt verzenden. De verbinding met Secumail en de ontvanger is gegarandeerd versleuteld. Als we geen veilige verbinding kunnen opbouwen dan leveren we niet af. Hiermee voldoe je als bedrijf of organisatie aan de eisen van de GDPR.

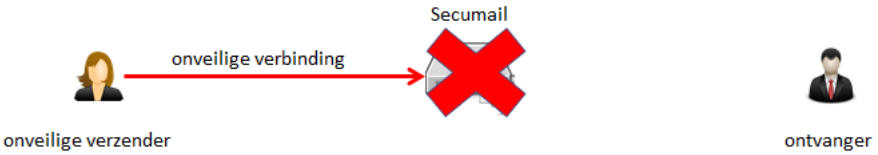
Als we de e-mail niet kunnen afleveren dan stellen we je daar als verzender van op de hoogte, zodat je op een alternatieve manier kunt communiceren.

Elke e-mail die we versturen via Secumail wordt digitaal gesigneerd waardoor de inhoud van het bericht niet veranderd kan worden. We leveren de e-mail af in de inbox van de ontvanger en monitoren of de aflevering correct verloopt.

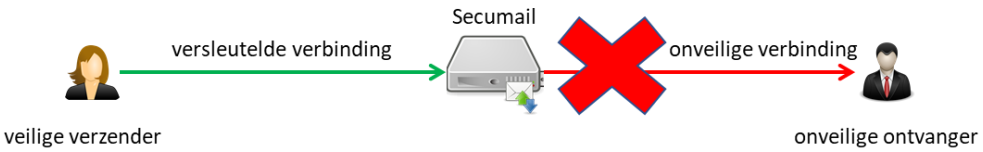
Zo werkt Secumail

Het basisprincipe van Secumail is heel eenvoudig We controleren zowel bij de verzender als bij de ontvanger of we een versleutelde verbinding kunnen opzetten. We gebruiken hiervoor de wereldwijde TLS standaard die tevens gebruikt wordt door banken, overheden en veiligheidsorganisaties.

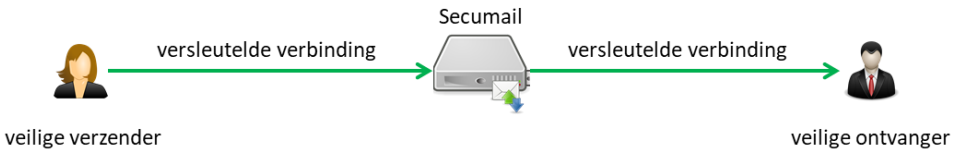
Stap 1 → Controleer de verzender Als eerste controleren we of de verzender versleuteld met ons communiceert. Dit kan in principe niet fout gaan omdat we eerst vaststellen of een nieuwe klant (=verzender) een versleutelde verbinding naar ons kan opzetten. Het kan echter voorkomen dat er in de toekomst iets fout gaat aan de verzendende kant, bijvoorbeeld een vervallen cryptografische sleutelset, zodat we dit continue blijven monitoren en onze klant op de hoogte brengen van eventuele issues.



Stap 2 → Controleer de ontvanger De volgende stap is dat we vaststellen of de ontvangende partij een versleutelde verbinding kan opzetten. Als dit niet lukt of als de versleutelde verbinding niet beantwoordt aan onze veiligheidseisen dan zullen we de e-mail niet afleveren en de verzender daarvan op de hoogte stellen.



Stap 3 → Digitale handtekening en aflevering Als aan alle veiligheidseisen is voldaan dan wordt de e-mail digitaal gesigneerd en afgeleverd bij de ontvanger. We houden de aflevering in de gaten en melden het als de ontvangende partij de e-mail weigert.



Is mijn mail server veilig?

Je kunt het makkelijk zelf controleren door een e-mail naar test@secumail.nl te sturen. Als je (verzendende) mail server een beveiligde verbinding aan kan bieden krijg je van ons een e-mail bevestiging. Zo niet dan krijg je een foutmelding. Zie je niets kijk dan in je Spam folder of bij “Onbelangrijke e-mail” als je Office 365 gebruikt.

Digitale handtekening

is een methode voor het bevestigen van de juistheid van digitale informatie door middel van bijvoorbeeld technieken van de asymmetrische cryptografie, op een wijze vergelijkbaar met het ondertekenen van papieren documenten aan de hand van een geschreven handtekening.

De technologie en beveiliging van Secumail

Secumail gebruikt baanbrekende, innovatieve technologie gebaseerd op de modernste cloud technologie van Amazon, serverless computing en event based computing. We voldoen aan de meest stringente eisen op het gebied van e-mail beveiliging en we werken conform ISO 27001/27002:2013 en NEN 7510.

Compliancy
Secumail werkt met de meest recente informatiebeveiligings-standaarden NEN 7510 en ISO 27001/27002:2013.

Data provenance
We werken uitsluitend met in Europa gevestigde datacenters, die volledig gecertificeerd zijn voor informatiebeveiliging (ISO27001, ISAE3402) en die goedkeuring hebben ontvangen van de Europese Unie voor het verwerken van persoonsgegevens van EU burgers.

Integratie
Secumail beschikt over standaard integraties voor Office 365, Exchange, alle gangbare Unix mailservers en Salesforce. We hebben een REST API beschikbaar voor applicatie integratie.

Cloud technologie stelt ons in staat binnen milliseconden te schalen van enkele e-mails naar miljarden e-mails zonder enige aanpassing aan onze infrastructuur of onze software. We kunnen elk volume verwerken, er zijn geen beperkingen qua capaciteit en er hoeven ook geen afspraken van te voren gemaakt te worden over wat er wel of niet aan capaciteit nodig is.

Serverless computing betekent dat we voor élke e-mail een eigen container (virtuele server) opstarten die we, nadat de e-mail verwerkt is, vervolgens vernietigen zodat er geen enkel digitaal spoor achterblijft. Er is geen enkele partij in de markt die dit niveau van databeveiliging kan evenaren.

E-mail beveiliging is onze kerncompetentie. We gebruiken onder andere de volgende standaarden in ons platform: TLS, PGP/MIME, SPF, DKIM, DMARC, MTA STS, TLSRPT, OpenID Connect en OAuth 2. Secumail werkt met een gesloten netwerk waarbij uitsluitend e-mails van geregistreerde en geverifieerde accounts worden verwerkt. Secumail controleert alle verwerkte e-mails op virussen en spam.

Public Key Infrastructure
Het cryptografisch sleutelmateriaal en Certificaat Autoriteit (CA) van Secumail is onder toezicht van een Nederlandse notaris op een Hardware Security Module gegenereerd. Dit proces is formeel vastgelegd en is verifieerbaar.

Elke keer als we een e-mail afleveren verifiëren we dat de verzender een versleutelde verbinding heeft gebruikt en dat de ontvangende partij een beveiligde verbinding aanbiedt. We controleren daarbij tevens dat de beveiligde verbinding is opgezet op basis van cryptografisch sleutelmateriaal van een vertrouwde basiscertificeringsinstantie.

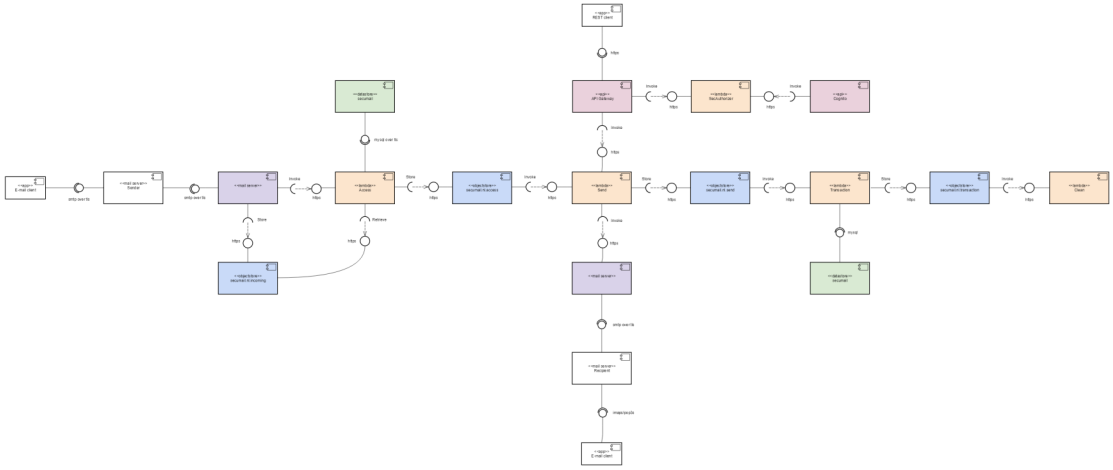
Ervaring
Het team van Secumail heeft tientallen jaren ervaring in het ontwerpen, bouwen en managen van online banken en wereldomspannende veilige e-mail systemen. Onze specialisten zijn CISSP en ISSAP gecertificeerd.

Secumail architectuur

Secumail maakt gebruik van een Staged Event Driven Architecture (SEDA) Elke e-mail binnen het systeem is een event emitter die de volgende stap in het proces triggert (asynchroon). Nieuwe stappen kunnen in het proces toegevoegd worden zonder software aanpassingen. Deze architectuur is vrijwel ongelimiteerd schaalbaar.

SEDA

The staged event-driven architecture (SEDA) refers to an approach to software architecture that decomposes a complex, event-driven application into a set of stages connected by queues. It avoids the high overhead associated with thread-based concurrency models (i.e. locking, unlocking, and polling for locks), and decouples event and thread scheduling from application logic. By performing admission control on each event queue, the service can be well-conditioned to load, preventing resources from being overcommitted when demand exceeds service capacity [bron: Wikipedfia]



Secure Gateways vormen de ingang en uitgang van het SEDA systeem. Binnen de Secure Gateway vindt TLS verwerking, access control en proces initiatie plaats.

De **API Gateway** vormt de toegang tot onze REST/JSON API. De API is formeel gedefinieerd in Open API Schema (Swagger).

Alle data gerelateerde services zijn geïsoleerd via **Virtual Private Clouds** (VPC).

Micro services vormen de elementaire processing units van het systeem op basis van volledige proces isolatie. De micro services worden los van elkaar ontwikkeld, getest en gedeployed.

Lambda containers vormen de run time omgeving. Voor elk event wordt een container binnen milli seconden gestart en na afloop van de verwerking vernietigd. Er kunnen daardoor nooit digitale sporen achterblijven.