Veilig mailen in het onderwijs

De Algemene Verordening Gegevensbescherming (AVG) stelt eisen ten aanzien van de bescherming van persoonsgegevens. In een toelichting van de Autoriteit Persoonsgegevens (AP) staat dat mailen van persoonsgegevens is toegestaan, maar dat dit dan wel veilig moet gebeuren[1]. Dit betekent dat je 'passende technische en organisatorische maatregelen' moet nemen. Deze maatregelen moeten de kans op een datalek verkleinen. Er is sprake van een datalek als persoonsgegevens bij de verkeerde persoon terechtkomen.

Vier belangrijke oorzaken van een datalek bij het mailen zijn:

- berichten die per ongeluk naar de verkeerde persoon verstuurd worden;
- verkeerde bestanden die per ongeluk als bijlage worden meegestuurd;
- e-mailboxen die worden gehackt, waarbij bijvoorbeeld een doorstuurregel wordt ingesteld;
- onveilige verbindingen waardoor verzonden berichten worden onderschept.

Welke toepassingen zijn veilig in gebruik en tegelijk ook gebruikersvriendelijk voor het onderwijs?
Door Privacy op School is een vergelijking gemaakt tussen een aantal toepassingen voor veilig mailen. Hierbij is onder andere gekeken naar:

- hoe de gegevens worden verstuurd en of versleuteling mogelijk is;
- welke normeringen van toepassing zijn;
- of de toepassing te integreren is in een bestaande e-mailapplicatie (Outlook, Gmail).

Versleuteling

Bij alle vergeleken toepassingen is het mogelijk om de e-mails te versleutelen. Versleutelen heeft als doel dat het bericht inclusief bijlage 'ongeopend' bij de ontvanger terecht komt en meegestuurde bijlages niet 'onderweg' (bijvoorbeeld op een openbaar wifi-netwerk) kunnen worden gelezen of worden aangepast. In combinatie met 2-factor authenticatie is dit de veiligste manier voor het versturen van e-mails naar (externe) ontvangers.

Bij 2-factor authenticatie (2FA) kun je een e-mail versleuteld versturen, waarbij de ontvanger de e-mail alleen kan openen als deze hiervoor ook een tweede middel (factor) tot zijn/haar beschikking heeft. Dit is vaak een code (sleutel) die apart wordt verstuurd of via een smartphone of token kan worden gegenereerd. Met deze sleutel kan het bericht dus leesbaar worden gemaakt voor de ontvanger.

Versleuteling van e-mail is alleen veilig wanneer de mailserver van de ontvanger ook deze versleuteling gebruikt, anders kan de e-mail alsnog niet-versleuteld worden verzonden[2]. Bij de meeste toepassingen kun je de toegang tot het bericht intrekken na het verzenden.

[1] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens
[2] Bij TLS-versleuteling wordt een mail alsnog onbeveiligd verstuurd, wanneer de ontvanger het versleutelde bericht niet kan openen, dit gebeurt niet bij end-to-end versleuteling).

Normeringen

De NTA 7516[3] is een normering die al toegepast wordt in de zorg voor het veilig uitwisselen van persoonlijke gezondheidsinformatie door zorgprofessionals. Leveranciers die voldoen aan de eisen die NTA 7516 stelt, laten zien dat ze de bescherming van privacy hoog in het vaandel hebben staan. De Autoriteit Persoonsgegevens (AP) heeft aangegeven het NTA7516 normenkader als een toetsingskader te zien als hiertoe aanleiding is. De toepassingen die deze norm hebben zijn in ieder geval veilige keuzes.

Daarnaast hebben we gekeken welke andere certificeringen voor informatiebeveiliging de applicaties hebben:

- ISO 27001 noemt de eisen voor het binnen de context van de organisatie vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging.
- NEN 7510 geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie moeten treffen ter beveiliging van de informatievoorziening.

Integratie en gebruiksgemak

Voor gebruiksgemak is het belangrijk dat een toepassing kan worden geïntegreerd in de huidige e-mailapplicatie, denk aan bijvoorbeeld Outlook en Gmail. Dit heeft over het algemeen de voorkeur ten opzichte van een (aparte) webapplicatie.
Daarbij kunnen toepassingen ook menselijke fouten reduceren door het toevoegen van onder meer het herkennen van sleutelwoorden en controle op de ontvangers. Verzenders worden dan gewaarschuwd als ze gevoelige gegevens e-mailen of e-mailen naar (voor het systeem) onbekende of externe ontvangers.

Vergelijking toepassingen voor veilig mailen

In het overzicht op de volgende pagina zijn de verschillende toepassingen voor veilig mailen met elkaar vergeleken. Er is hierbij gekeken naar de toepassingen die wij - Privacy op School - het meest tegenkomen in het onderwijs. De lijst is dus zeker niet uitputtend. De peildatum voor de prijs is december 2020. We raden aan om altijd actuele (prijs)informatie op te vragen bij de leverancier.

[3] https://www.nen.nl/nta-7516-2019-nl-254878

	End-to-end	TLS beveiliging[4]	Web applicatie	Integratie met ander mailpapplicatie	Verwerkers overeenkomst	2-factor authenticatie	Code via ander kanaal	Volgen mail	Link delen i.p.v. mailen	Herkenning sleutelwoord	Prijs[5]	NTA 7516 nomering	ISO 27001 / NEN 7510
Outlook Microsoft 365	j	j	j	nvt	j	j	j	j	j	n	€0,00	n	j
Google		j	j	nvt	j	j	j	j	n	n	€0,00	n	j
Zivver	j	j	j	j	j	j	j	j	n	j	€9,98	j	j
Zorgmail	j	j	j	j	j	j	j	j	n	j/n	€1,47	j	j
SMARTLOCKR	j	j	j	j	n[6]	j	j	j	j	j	€4,20	j	j
Aangetekend mailen	j		j	j	j	j	j	j	n	n	€6,05	j	j
FileCap	j		j	j	j[7]	j	j	j	j	j	€5,95	n	j
Skotty	j		j	n	j	j	j	j	n	n	€7,00	n	n
Skotty Blocks	j		j	j	j	j	j	j	j	n	€1500[8]	n	n
SURFFilesender	j		j	n	n	j	j	j	n	n	€0,00[9]	n	n

Op de volgende pagina's wordt per toepassing een nadere toelichting gegeven.

[4] SMARTLOCKR geeft aan dat zij geen verwerker zijn.
[5] Kan on premise (en in de cloud.)
[6] Voor 2 jaar, onbeperkt aantal gebruikers en opslag.
[7] Gratis indien aangesloten op het SURF-netwerk.
[8] Prijzen per gebruiker/per maand bij 50 gebruikers, peildatum december 2020.
[9] Bij TLS-versleuteling wordt een mail in principe beveiligd verstuurd. Wanneer de ontvanger het versleutelde bericht niet kan openen, wordt deze alsnog niet-versleuteld verstuurd (dit gebeurt niet bij end-to-end versleuteling).

Microsoft365

Wanneer je in Microsoft365 berichtversleuteling wilt gebruiken, moet je een Office 365 E3 licentie hebben. Het pakket (add-in) is gratis, maar moet wel in Azure Information Protection (AIP) worden aangezet. Binnen Microsoft365 heb je dan de mogelijkheid om berichten te versleutelen (encryptie). Verder is er ook nog de mogelijkheid om het doorsturen, kopiëren en afdrukken te beperken. En is er de mogelijkheid om aan te geven dat een mail 'bedrijfsvertrouwelijk' is, waardoor e-mail niet naar personen buiten de organisatie kan worden verstuurd.

Dat werkt allemaal redelijk voor de verzender. Voor de ontvanger is het afhankelijk welke e-mail applicatie wordt gebruikt. Wanneer dit geen Microsoft365 is, dan moet de ontvanger extra handelingen doen om de e-mail te lezen: een eenmalige code aanvragen (of aanmelden met account i.g.v. Google) die moet worden ingevoerd. Deze vorm van versleuteling voorkomt niet dat onbevoegden toegang krijgen tot de informatie wanneer het e-mailaccount is gehackt.

Een andere, en naar onze mening, goede manier van het veilig uitwisselen van gegevens buiten de organisatie is het delen van een bestand. Dit kan door een link naar het bestand te mailen naar de ontvanger. Deze link wordt ingesteld met de optie 'Iedereen met de koppeling', maar dan wel gecombineerd met een wachtwoord! Bij deze mogelijkheid heb je tevens de opties om een datum in te stellen wanneer de toegang tot het document verloopt en of je het downloaden van het document toestaat. Deze manier werkt zowel vanuit Outlook als vanuit een geopend office document.

Het voordeel van deze aanpak is dat de verzender controle houdt over het document, de toegangsrechten op ieder moment eenvoudig kan intrekken en het document niet wordt gedupliceerd. Uiteraard moet het wachtwoord dan wel via een ander kanaal naar de ontvanger worden gestuurd (bijvoorbeeld per SMS)!
Zie ook de gratis poster op onze website over 'veilig delen' met een instructie hoe je dat doet.

Google

Binnen Gmail is er ook een gratis mogelijkheid om veilig te e-mailen, door de optie 'vertrouwelijke modus' in te stellen. Je kunt hiermee een wachtwoord instellen en voorkomen dat de e-mail wordt doorgestuurd, wordt gekopieerd of wordt gedownload. Ook kan je een datum instellen waarop de e-mail verloopt. Ontvangers moeten zich hiervoor wel bij Google aanmelden. Dit kan een probleem zijn wanneer de ontvanger geen Google account heeft. Via MijnDrive is het ook mogelijk om documenten te delen in plaats van te e-mailen. Ook hier kun je een datum instellen dat de toegang verloopt.

Zivver

Zivver kan worden geïntegreerd met Outlook, Gmail, EDP, HRM. Je krijgt dan een extra knop in je mailomgeving. Zivver heeft een NTA7516 certificering en voldoet hiermee aan de hoogste standaard voor veilig e-mailen. In de applicatie zijn diverse beveiligingscontroles ingebouwd: herkenning van sleutelwoorden en controle van ontvangers waardoor voor het versturen van een e-mail je wordt geattendeerd op mogelijke in te stellen veiligheidsmaatregelen en lijkt eenvoudig in gebruik.
N.B. boven 50 gebruikers biedt Zivver maatwerk en mogelijk een betere prijs per gebruiker.

Zorgmail

Zorgmail wordt volop (de naam zegt het al) in de zorg gebruikt. Zorgmail heeft een add-in beschikbaar waarmee een "Veilig Verzenden" knop wordt toegevoegd aan Outlook. De standaard is dat de e-mail altijd veilig wordt verstuurd en dat de verzender dit uit kan zetten als dat niet nodig is. Ook Zorgmail heeft een NTA7516 certificering en voldoet hiermee aan de hoogste standaard voor veilig e-mailen. Er was ook een herkenning van sleutelwoorden en controle van ontvangers

ingebouwd, maar dit hebben ze in de laatste versie er weer uitgehaald op basis van minder positieve klantervaring. Door het invoeren van het gsm-nummer van de ontvanger kan deze een verificatiecode op dat nummer krijgen. Wanneer geen nummer wordt ingevoerd, wordt een code gemaild. Nadat een e-mail veilig is verstuurd, kan deze niet meer worden teruggehaald, eventueel kan er wel een vertraging worden ingesteld in het daadwerkelijk verzenden. Zorgmail is per gebruiker erg goedkoop, maar rekent wel € 1042,- voor onboarding, inclusief een sms bundel. De prijs in de tabel is voor 50 gebruikers, de bundel die zorgmail biedt is tot 100 gebruikers, dus in dat geval € 0,73 per gebruiker.

SMARTLOCKR

SMARTLOCKR kan eveneens worden geïntegreerd met Outlook en daarmee krijg je een extra knop in je e-mailomgeving. Op termijn komt er ook een integratie met Gmail. Ook SMARTLOCKR heeft een NTA7516 certificering en voldoet hiermee aan de hoogste standaard voor veilig e-mailen. De applicatie probeert de menselijke fouten zoveel mogelijk te filteren door het herkennen van sleutelwoorden, waarna suggesties worden gegeven over de beveiliging. Verzonden berichten kunnen ook worden gevolgd en toegang kan na verzenden worden ingetrokken. Deze applicatie lijkt eenvoudig in gebruik. Het meest uitgebreide pakket kost € 4,20 per gebruiker per maand, dit is exclusief € 2.400 voor on-boarding, installatie en uitleg.

Aangetekend mailen

Aangetekend mailen kan eveneens worden geïntegreerd met Outlook. Daarmee krijg je een extra knop in je e-mailomgeving. Op termijn komt er ook een integratie met Gmail. Ook Aangetekend mailen heeft een NTA7516 certificering en voldoet hiermee aan de hoogste standaard voor veilig mailen. Het proces van versturen kan door de verzender worden gevolgd.

FileCap

FileCap kan worden geïntegreerd met Outlook, maar nog niet met Gmail. De applicatie kan zowel ‘on premise’ en als een cloudomgeving worden aangeboden. De prijs is inclusief installatie, on-boarding en een testmaand. Je hebt een keuze voor een abonnement van 1, 3 of 5 jaar. FileCap heeft nog geen NTA7516 certificering, zij verwachten een audit in januari 2021 aan te kunnen vragen (voor de hosting oplossing).

Skotty / Skotty Blocks

Skotty is een webapplicatie dat niet kan worden geïntegreerd in andere applicaties. Via WhatsApp of e-mail kan een code worden gestuurd, waarna de ontvanger het bericht kan openen.

Skotty is bezig met een nieuwe applicatie die wel is te integreren met Outlook: Skotty Blocks. Deze oplossing wordt nog niet als pakket aangeboden (verwachting vanaf Q2-2021), maar vooralsnog alleen nog als maatwerkoplossing. Skotty Blocks heeft nog geen NTA7516 certificering, maar verwacht een audit in Q2-2021 aan te kunnen vragen (voor de hosting oplossing). De prijs van € 1.500 is voor een abonnement van 2 jaar. Dit is voor een onbeperkt aantal gebruikers en opslag.

SURF Filesender

SURF Filesender is een open source webapplicatie. Bestanden worden end-to-end versleuteld. De bestanden zijn beschikbaar voor een beperkte tijd en een beperkt aantal ontvangers, naar keuze van de afzender. Daarna worden de bestanden automatisch uit de applicatie verwijderd. SURF FileSender is snel, gebruiksvriendelijk en kan bestanden van elke grootte aan. SURF Filesender is gratis indien de organisatie is aangesloten op het SURF-netwerk.