Bijlage 2

SECURITY & PRIVACY ASSESSMENT VIDEO VERGADERTOOLS

Het Waterschapshuis

SECURITY & PRIVACY ASSESSMENT VIDEO VERGADERTOOLS

Het Waterschapshuis

Floris Baauw, Manisha Ramsaran

DATUM	**6-5-2020**
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20207536
INTERNE TOETS	Monica de Wit

ONS ADVIES

Op basis van onze analyse van de vergadertools op security en privacy aspecten adviseren wij de Webex tool van Cisco te gebruiken. Op zowel security als privacy gebied komt deze tool wat ons betreft het beste naar voren.

De tool biedt uitgebreide mogelijkheden om security naar voorkeur in te stellen, onder andere op het gebied van toegangsbeveiliging, versleuteling van datastromen, vergaderinstellingen die per vergadering aanpasbaar zijn en mogelijkheden tot privacy vriendelijke instellingen van vergadersessies. De mogelijkheden die Webex biedt aan gebruikers op het gebied van security bewijst dat Webex security zeer belangrijk vindt. Relevante certificeringen als ISO27001 en SOC 2 type II ondersteunen dat beeld. Op het gebied van haar security onderscheidt Webex zich dus vooral in het aantal mogelijkheden en de invloed die je als gebruiker kunt hebben op de mate van security. Daarnaast verwerkt Webex met name functioneel noodzakelijke gegevens en is het bedrijf transparant over haar verwerkingsdoeleinden. Vergeleken met Zoom, MS Teams & Google Meet scoort Webex beter op verenigbaar gebruik in de praktijk. Tenslotte worden gespreksgegevens, in tegenstelling tot de meeste andere tools, in Nederland opgeslagen.

Hierbij merken wij wel op dat de Webex vergadertool op basis van de voorgaande analyse niet noodzakelijk veel beter uit de vergelijking komt dan tools als MS Teams, Starleaf en Google Meet. Op hoofdlijnen zijn deze tools namelijk vergelijkbaar. Webex scoort op dit moment alleen duidelijk beter dan Zoom in onze vergelijking. Onze voorkeur voor Webex wordt gedreven door een combinatie van de mogelijkheid tot security- en privacy vriendelijke maatregelen, transparantie over haar toegang tot data van klanten en de Role Based Access Control (RBAC) die de supportafdeling hiervoor gebruikt. Daarnaast biedt Webex de mogelijkheid tot end-to-end encryptie, als de gebruiker accepteert dat er dan minder functionaliteiten beschikbaar zijn. Op basis van de analyse van de tools lijkt de regie op het gebied van security en privacy bij de Webex tool meer in handen van de gebruiker te liggen dan bij de andere tools.

Onderstaande tabel geeft een overzicht van hoe de tools scoren op de door VKA opgestelde criteria. Hierbij staat een '–' voor onvoldoende, '+/-' voor matig, '+' voor goed en '++' voor uitstekend.

	Zoom	Webex	MS Teams	Starleaf	Google Meet
1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt	+	+	+	+	+
2. Elektronische communicatie beschermen	+/-	++	+	+	+
3. Leverancier is 'security-minded' in haar dienstverlening	+	++	+	+	+
4. De leverancier voldoet aan relevante security normen	+	++	++	++	++
5. Verzameling van minimaal aantal gegevens	+	+	-	+	-
6. Gebruik voor gerechtvaardigde doeleinden	-	+	-	-	-
7. Passend beschermingsniveau	+	+	+	+	+

Naar aanleiding van een aanvullende vraag van HWH, adviseren wij de volgende mogelijke vervolgstappen:

- Aanvullend onderzoek naar de security en privacy mogelijkheden van Webex voor een optimale configuratie, waarmee de organisatie verzekert dat zij de mogelijkheden tot gegevensbescherming van de tool optimaal benut.
- Ontwikkeling van een algemene gebruikersinstructie van vergadertools, gericht op security en privacy aspecten.
- Ontwikkeling van een Webex-specifieke gebruikersinstructie, zowel voor 'admins' en 'hosts' als de gewone gebruiker
- indien mogelijk en nog niet verricht; een verwerkersovereenkomst met de leverancier afsluiten. Daarmee zijn de wederzijdse verplichtingen aantoonbaar afgedekt.

INHOUDSOPGAVE

Ons advies **3**

Inhoudsopgave **5**

1 Inleiding **6**
1.1 Achtergrond 6
1.2 Vraagstelling 6
1.3 Doel van dit document 6

2 Criteria analyse video vergadertools **7**
2.1 Security en Privacy criteria 7

3 Analyse video vergadertools **9**
3.1 Zoom 9
3.2 Webex 10
3.3 MS Teams 12
3.4 Starleaf 13
3.5 Google Meet 14

4 Advies verstandig gebruik video vergadertools **16**

A Bijlage A - bronnen **18**

1 INLEIDING

1.1 Achtergrond

Het Waterschapshuis (HWH) heeft van de Vereniging van Directeuren van de 21 Waterschappen (VDW) en van de Unie van Waterschappen (UVW) de vraag gekregen 1) een inventarisatie uit te voeren op het gebruik van video vergadertools door waterschappen en 2) een afwegingskader te maken op de keuze van een waterschap voor een video vergadertool en 3) een advies uit te brengen op de keuze voor een video vergadertool voor communicatie tussen waterschappen en tussen waterschappen en derde partijen. HWH heeft een projectgroep geformeerd om dit advies te kunnen verzorgen.
Bij dit advies wegen ook security- en privacyaspecten zwaar mee. Op dit moment zijn er vijf vergadertools aangewezen die passend lijken voor het Waterschapshuis: Zoom, Webex, MS Teams, Starleaf en Google Meet.

1.2 Vraagstelling

De projectgroep heeft aan VKA gevraagd een adviesrapport op te stellen, opgedeeld in drie onderdelen:

1. een security en privacy analyse van de genoemde vergadertools;
2. een advies gericht op verstandig gebruik van deze tools vanuit security en privacy perspectief;
3. een conclusie; welke vergadertool komt, gekeken naar security en privacy aspecten, het beste uit de bus.

1.3 Doel van dit document

Dit document voorziet het Waterschapshuis van een advies welke van de vijf genoemde vergadertools op het gebied van security en privacy de beste keuze zou zijn. Het Waterschapshuis neemt dit advies vervolgens mee in haar overweging welke video vergadertool zij voor de gehele organisatie aanbeveelt.

2 CRITERIA ANALYSE VIDEO VERGADERTOOLS

2.1 Security en Privacy criteria

Om te kunnen beoordelen welke video vergadertool het beste past bij HWH heeft VKA een aantal security- en privacy criteria opgesteld, gebaseerd op normen uit de Baseline Informatiebeveiliging Overheid (BIO) en Algemene Verordening Gegevensbescherming (AVG):

1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt
Toegang tot de vergadertool, met daarin informatie en systeemfuncties van toepassingen behoort te worden beperkt (BIO, HS. 9). Dit verhindert dat onbevoegden zich toegang kunnen verschaffen tot de vergadersessies. Toegangsbeperking kenmerkt zich door: 1) mogelijkheid tot beveiligde inlogprocedures (twee-factor een pré), 2) gebruik sterke wachtwoorden (afgedwongen), 3) beheerders hebben grip op toegang tot vergaderingen (toestemming voor toegang vereist, lobby-functie).

2. Elektronische communicatie beschermen
Informatie die is opgenomen in elektronische communicatie behoort passend te zijn beschermd (BIO, HS. 13). Dit voorkomt dat onbevoegden zich toegang kunnen verschaffen tot de elektronische communicatie. Passende bescherming kenmerkt zich door: mogelijkheid tot een vorm van encryptie (bijv. end-to-end).

3. Leverancier is 'security-minded' in haar dienstverlening
De leverancier behoort aan alle relevante informatiebeveiligingseisen te voldoen, aangezien de leverancier toegang heeft tot de elektronische communicatie van de organisatie of deze verwerkt of opslaat (BIO, HS. 15). Duidelijke afspraken op dit gebied zorgen ervoor dat de leverancier op een veilige en (privacy) verantwoorde manier met de informatie, voortkomend uit de vergadersessies, omgaat. Relevante informatiebeveiligingseisen kenmerken zich door: 1) de leverancier slaat geen gegevens van de organisatie op (of verwijdert deze direct na een vergadersessie), 2) de leverancier verschaft zichzelf op geen enkel moment toegang tot de (informatie uit) vergadersessies, 3) de leverancier heeft een (security) incidenten procedure en kan hierdoor goed omgaan met kwetsbaarheden.

4. De leverancier voldoet aan relevante security normen
Dit is aantoonbaar en terug te zien in het handelen van de leverancier (BIO, HS. 18). Het voldoen van de leverancier aan een bepaalde security norm geeft een indicatie van het belang dat de leverancier hecht aan veilige dienstverlening en veronderstelt een zeker basisniveau van security. Relevante security normen zijn: 1) ISO27001, 27002, 27017 of 27018 certificering, 2) SOC 1/2 (type II).

5. Verzameling van minimaal aantal gegevens
Uit het beginsel van gegevensminimalisatie vloeit voort dat niet meer gegevens dan noodzakelijk verzameld mogen worden voor het na te streven doel (art. 6 lid 1 sub c AVG). Hiermee wordt voorkomen dat de leverancier onnodig veel gegevens verzamelt. Relevante factoren zijn o.a.: 1)

categorieën persoonsgegevens: algemeen, gevoelig (onder striktere voorwaarden) & bijzonder (niet gewenst), 2) verwerking ziet met name op functioneel noodzakelijke gegevens, bijvoorbeeld contact- en locatiegegevens, 3) de hoeveelheid te verwerken gegevens is beperkt tot een noodzakelijk minimum.

6. Gebruik voor gerechtvaardigde doeleinden

Op grond van het beginsel van doelbinding moet de leverancier heldere, vastomlijnde doeleinden omschreven hebben om gegevens te mogen verwerken (art. 6 lid 1 sub c AVG). Voor gebruikers moet het inzichtelijk zijn wat er precies met hun persoonsgegevens gebeurt. Hierbij wordt rekening gehouden met: 1) duidelijk geformuleerde doeleinden in het privacy statement, 2) hangen bepaalde doeleinden, bijvoorbeeld commercieel van aard, samen met gegevensverstrekking aan derde partijen? (bij voorkeur beperkt), 3) aantoonbaar verenigbaar gebruik in de praktijk (zijn situaties bekend waarin de leverancier afwijkt van de oorspronkelijk geformuleerde doeleinden?)

7. Passend beschermingsniveau

Het is inzichtelijk onder welk privacy-regime een leverancier valt en of een passend beschermingsniveau gewaarborgd kan worden (art. 46 AVG). Leveranciers buiten Europa vallen niet direct onder de 'strenge' Europese wetgeving en moeten kunnen aantonen dat ze op vergelijkbare wijze veilig gegevens uitwisselen. Belangrijke criteria zijn: 1) het hoofdkantoor van de leverancier is bij voorkeur binnen de EU gevestigd, i.v.m. toepasselijke privacywetgeving en dataopslag, 2) de gegevens worden bij voorkeur in Nederland of een ander Europees land opgeslagen, i.v.m. toepasselijke privacywetgeving en dataopslag 3) indien sprake is van dataopslag in een niet-Europees land zijn waarborgen getroffen om een adequaat beveiligingsniveau te garanderen, bijvoorbeeld door een Privacy Shield certificering of het gebruik van modelcontracten.

3 ANALYSE VIDEO VERGADERTOOLS

In dit hoofdstuk zijn de door HWH aangewezen video vergadertools geanalyseerd op basis van de 7 security- en privacy criteria uit hoofdstuk 2.

3.1 Zoom

1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt

Zoom biedt een aantal waardevolle mogelijkheden tot toegangsbeveiliging. Allereerst is het mogelijk in te loggen met Single Sign-On. Daarnaast kunnen vergadersessies beveiligd worden met een wachtwoord (pincode) en is het mogelijk een wachtruimte in te stellen voor deelnemers aan de vergadering. Zoom biedt geen directe mogelijkheid tot tweefactor authenticatie. Het is wel mogelijk Zoom te integreren in bijvoorbeeld het Active Directory (AD) van een organisatie en op deze manier tweefactor authenticatie af te dwingen.

2. Elektronische communicatie beschermen

Om de elektronische communicatie van gebruikers te beschermen biedt Zoom 256-bit TLS encryptie. Sinds de update naar Zoom 5.0 is daar sinds kort ook AES-256 encryptie aan toegevoegd. In de praktijk betekent dit dat gesprekken (gesproken of in chat) met 265-bit TLS encryptie worden beschermd. Elke andere vorm van informatie die via de Zoom vergadersessies wordt gedeeld kan met AES-256 encryptie worden beschermd. De AES-256 encryptie staat bekend als een betere vorm van encryptie dan de 265-bit TLS encryptie. Voor beide vormen van encryptie geldt dat het niet gaat om end-to-end encryptie. Daarnaast blijkt tot nu toe dat een onder andere door het NCSC erkende kwetsbaarheid in de versleuteling van Zoom nog niet is opgepakt in de 5.0 update.[2]

3. Leverancier is 'security-minded' in haar dienstverlening

Zoom zegt op haar website dat haar medewerkers zich op geen enkel moment toegang verschaffen tot vergadersessies van haar klanten. In de afgelopen tijd is hier wel controverse over geweest, omdat bleek dat Zoom gegevens van haar klanten deelde met onder andere Facebook.[3] Zoom heeft echter haar beleid aangepast en zegt nu alleen vanuit een service gerichte rol vergadersessies te monitoren. Hierbij verschaffen zij zich geen toegang tot eventuele content die in een vergadering wordt gedeeld. Zoom slaat wel gegevens op van haar klanten. Het gaat dan om accountgegevens en opnames van vergaderingen die op de Zoom Cloud worden opgeslagen, indien de gebruiker hiervoor kiest.

4. De leverancier voldoet aan relevante security normen

Zoom voldoet aan de SOC 2 type II norm. SOC is een Amerikaanse norm van AICPPA, in eerste instantie vooral bedoeld voor finance control. SOC 2 type II biedt ook security controls voor Cloud Service Providers en is daarom een relevante security norm. Zoom geeft op haar site aan deze norm te volgen, maar licht verder niet toe op welke gebieden zij dat doet en of een certificaat is behaald.

5. Verzameling van minimaal aantal gegevens

Zoom verzamelt voornamelijk algemene persoonsgegevens die functioneel noodzakelijk van aard zijn en daarnaast gegevens van meer gevoelige aard, waaronder (metadata van) gespreksgegevens. Exacte locatiegegevens worden niet getrackt. Optioneel verwerkt de app opgegeven bedrijfsgegevens, telefoonnummer en profielfoto.

6. Gebruik voor gerechtvaardigde doeleinden

Het verbeteren van de app is een van de doeleinden voor gegevensverwerking (met geanonimiseerde/geaggregeerde technische gegevens en gegevens hoe de app gebruikt wordt). Zoom zegt geen persoonsgegevens door te verkopen of te gebruiken voor advertentie-doeleinden. In het verleden bleek het bedrijf niet transparant te zijn over het delen van analytische gegevens met Facebook. Dergelijke misstanden zijn – naar eigen zeggen- inmiddels verholpen.[5] Wel kan pas na uitvoering van bijvoorbeeld onafhankelijk onderzoek met zekerheid gezegd worden dat gegevens niet zonder meer naar derde partijen worden doorgespeeld voor andere doeleinden.

7. Passend beschermingsniveau

Het hoofdkantoor van Zoom is gevestigd in Californië, de Verenigde staten, waardoor het niet direct valt onder Europese wetgeving. Het bedrijf beschikt over een Privacy Shield certificering en maakt gebruik van modelcontracten. Dankzij een recente update kan een betalende gebruiker zelf kiezen op welke servers in bepaalde regio's de data opgeslagen wordt, waaronder dus Europa.

3.2 Webex

1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt

Webex biedt meerdere mogelijkheden tot toegangsbescherming. Net als Zoom maakt Webex gebruik van Single Sign-On. Deze inlogmethode is te koppelen aan de toegangsbeveiligingsmethode van klanten, zoals aan Active Directory. Aanvullend hierop maakt Webex het ook mogelijk Role-Based-Access-Control (RBAC) in te schakelen. Dit betekent dat er in de tool een aantal rollen zijn gedefinieerd, die security verantwoordelijkheden met zich meedragen. De toegevoegde waarde hiervan is dat medewerkers in de organisatie aangewezen kunnen worden als 'host' of 'administrator'. Alleen deze medewerkers hebben dan de bevoegdheid security instellingen aan te passen een kunnen hier op voorhand goed over geïnstrueerd worden. Eén van deze bevoegdheden is de mogelijkheid om het gebruik van sterke wachtwoorden bij alle gebruikers af te dwingen.

2. Elektronische communicatie beschermen

Webex biedt meerdere mogelijkheden als het gaat om het beschermen van elektronische communicatie. Organisaties kunnen namelijk zelf kiezen of zij end-to-end encryptie willen afdwingen voor elke vergadersessie, dit optioneel maken (dus de host van de sessie mag zelf kiezen) of end-to-end encryptie uitzetten. End-to-end encryptie aanzetten zorgt er namelijk voor dat een aantal functionaliteiten van de tool niet gebruikt kunnen worden, zoals het remote delen van een scherm of een persoonlijke meeting omgeving instellen. De standaard is dat de elektronische communicatie wordt versleuteld tot het bij Webex binnenkomt, dus versleuteling tijdens de stroom

van de gebruiker naar Webex en andersom. Webex gebruikt hier onder andere AES-256 encryptie voor, maar beperkt zich niet tot die vorm van encryptie.

3. Leverancier is 'security-minded' in haar dienstverlening

Webex slaat alleen gegevens op van haar klanten die nodig zijn voor het aanbieden van haar diensten. Vergelijkbaar met Zoom betekent dit dat accountgegevens (kunnen) worden opgeslagen. Het principe dat hierbij wel geldt, is dat Webex alleen datgene opslaat wat de gebruiker haar toestaat. Afhankelijk van de voorkeuren van een organisatie is het mogelijk om met Webex te werken zonder noemenswaardige gegevens te delen met het bedrijf. Indien Webex zichzelf toegang verschaft tot (data uit) vergadersessies, dan doen zij dit alleen vanuit een service-gerichte vraag van een klant. Hiervoor heeft Webex zelf ook RBAC ingesteld; alleen Webex medewerkers met de juiste toegangsrechten mogen toegang verkrijgen tot data van klanten (voortkomend uit een klantvraag). Deze medewerkers worden jaarlijks verplicht een security awareness training te volgen (ISO27001).

4. De leverancier voldoet aan relevante security normen

Webex is ISO27001 en SOC 2 type II gecertificeerd. Beiden zijn relevante security normen voor een dergelijke leverancier. Vooral een ISO27001 certificering is, gekeken naar BIO compliance in Nederland, interessant, omdat deze twee normen veel gelijkenissen tonen.

5. Verzameling van minimaal aantal gegevens

De app verzamelt voornamelijk functioneel noodzakelijke gegevens, waaronder betaal- en locatiegegevens (enkel geografische regio) en daarnaast gegevens van meer gevoelige aard, waaronder (omvangrijke metadata van) gespreksgegevens. Mailadressen, telefoonnummers en profielfoto's kunnen gebruikers optioneel verstrekken.

6. Gebruik voor gerechtvaardigde doeleinden

Webex gebruikt registratiegegevens en metadata van gespreksgegevens voor analyse-doeleinden. De gegevens worden in geaggregeerde vorm verwerkt en zijn dus niet volledig anoniem. Het bedrijf geeft aan geen persoonsgegevens door te verkopen voor commerciële doeleinden. Er zijn geen specifieke gevallen bekend waarin Webex hiervan af bleek te wijken.

7. Passend beschermingsniveau

Het hoofdkantoor van Webex is gevestigd in Californië, de Verenigde Staten, waardoor het niet direct valt onder Europese wetgeving. Het bedrijf beschikt over een Privacy Shield certificering en maakt gebruik van modelcontracten. Gespreksgegevens van Nederlandse gebruikers worden in Nederland opgeslagen. Betaal- en analytische gegevens slaat het bedrijf in de Verenigde Staten op.

3.3 MS Teams

1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt

Teams is onderdeel van de Office 365 omgeving. Hierdoor kan Teams ook gebruikmaken van de security oplossingen die de Office 365 omgeving biedt. Dit betekent voor toegangsbescherming dat Teams multi-factor authenticatie afdwingt voor alle gebruikers en daarnaast ook gebruik maakt van SSO via het Active Directory. Administrators van de eigen organisatie kunnen het gebruik van sterke wachtwoorden afdwingen en aanpassen aan de eisen van de organisatie.

2. Elektronische communicatie beschermen

Teams maakt gebruik van encryptie voor datastromen die verstuurd worden en data die 'stil staat'. In de praktijk betekent dit dat de data versleuteld is, tot het bij Microsoft binnenkomt en weer versleuteld wordt wanneer het Microsoft verlaat. Het gaat hier dus niet om end-to-end encryptie. Naast deze encryptie biedt Microsoft haar klanten vanaf de basis licentie al vormen van security oplossingen aan, die proactief monitoren op kwetsbaarheden.

3. Leverancier is 'security-minded' in haar dienstverlening

Microsoft zegt serieus om te gaan met de bescherming van data van haar klanten. Hiervoor heeft Microsoft onder andere Trust ontwikkeld. Dit is een onderdeel van Microsoft wat zich alleen bezighoudt met het garanderen van een hoog security en privacy niveau voor gebruikers. Het uitgangspunt van Microsoft is dat data van klanten alleen vanuit een service-gerichte vraag wordt benaderd en niet voor andere doeleinden. Om deze reden slaat Microsoft ook geen gegevens van haar klanten, voortkomend uit Teams vergadersessies, op. Documenten die worden gedeeld blijven op de omgeving (Tenant) van de klant staan. Een uitzondering hierop zijn opnamen van vergadersessies door gebruikers. Als een gebruiker een opname maakt, wordt die in de Cloud van Microsoft opgeslagen.

4. De leverancier voldoet aan relevante security normen

Microsoft heeft certificaten van meerdere relevante security normen: ISO27001, ISO27018, SOC 1 en SOC 2. De ISO27018 is een norm gericht op security voor Cloud providers met specifiek doel het beschermen van privacy van gebruikers.

5. Verzameling van minimaal aantal gegevens

De app verzamelt een groot aantal persoonsgegevens van gebruikers, die ook afkomstig kunnen zijn van derde partijen. Het generieke privacy statement voor alle Microsoftproducten benoemt niet specifiek welke gegevens Microsoft Teams verwerkt. Een oordeel of sprake is van minimale gegevensverwerking kan dus niet geveld worden.

6. Gebruik voor gerechtvaardigde doeleinden

Microsoft gebruikt verzamelde persoonsgegevens o.a. voor het verbeteren en ontwikkelen van hun producten, maar maakt niet duidelijk om welke gegevens dit precies gaat en in hoeverre ze wel/niet geanonimiseerd worden. Het bedrijf geeft aan geen persoonsgegevens uit Teams te gebruiken voor

commerciële doeleinden (advertenties). Wel koppelt Microsoft gegevens uit Teams met gegevens uit andere Microsoft producten, waardoor verenigbaar gebruik betwistbaar wordt.

7. Passend beschermingsniveau
Het hoofdkantoor van Microsoft is gevestigd in Washington, de Verenigde Staten, waardoor het niet direct valt onder Europese wetgeving. Het bedrijf beschikt over een Privacy Shield certificering. Gegevensopslag vanuit Microsoft Teams vindt voor Nederlandse gebruikers plaats in Dublin en Amsterdam.

3.4 Starleaf

1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt
Starleaf biedt de mogelijkheid tot toegangsbescherming. Dit doet zij op meerdere manieren. Gebruikers worden geacht een account aan te maken en hiermee in te loggen (SSO). Externe gebruikers worden via een mail uitgenodigd met een unieke code. Daarnaast kan de host van de vergadering deelnemers wel of niet toelaten tot de vergadering. Starleaf biedt zelf verder geen duidelijke inhoudelijke toelichting op hun oplossingen voor toegangsbescherming.

2. Elektronische communicatie beschermen
In haar Security Whitepaper biedt Starleaf een inkijk in de security oplossingen die Starleaf biedt voor haar videovergadering diensten. Ten opzichte van de andere leveranciers pakt Starleaf het net wat anders aan. Alle gebruikers van de tool (dus ook externe gebruikers) worden binnen de 'Starleaf Cloud' geplaatst. Dit zorgt ervoor dat er geen endpoints op een eigen onbeschermd privé netwerk data ontvangen en verzenden. Starleaf neemt hiermee organisaties het werk van het inrichten van VPN verbindingen voor dergelijke situaties uit handen. De elektronische communicatie wordt binnen de Cloud versleuteld verstuurd. Starleaf spreekt zelf alleen expliciet van een end-to-end encryptie als het gaat om 'private direct media' calls. Dit zijn videovergaderingen tussen twee collega's, die op hetzelfde netwerk werken. Voor haar verdere dienstverlening spreekt Starleaf van constante encryptie, maar noemt zij dit geen end-to-end encryptie. Het is met de beschikbare informatie niet te achterhalen welke vorm Starleaf hiervoor precies aanbiedt.

3. Leverancier is 'security-minded' in haar dienstverlening
Starleaf handelt op dit punt gelijk aan Teams, Webex en Meet. Opgenomen vergaderingen worden opgeslagen bij Starleaf. Starleaf kan toegang krijgen tot vergadersessies of individuele gebruikers, maar doet dit naar eigen zeggen alleen vanuit een service-gerichte vraag van de klant.
Starleaf licht zelf niet duidelijk toe of en wat haar incidenten procedure behelst, maar voldoet aan de ISO27001 norm. Incident management is hier een onderdeel van.

4. De leverancier voldoet aan relevante security normen
Starleaf is sinds vorig jaar ISO27001 gecertificeerd.

5. Verzameling van minimaal aantal gegevens

Starleaf verzamelt voornamelijk algemene persoonsgegevens die functioneel noodzakelijk zijn en daarnaast gegevens van meer gevoelige aard, waaronder (metadata van) gespreksgegevens. Exacte locatiegegevens worden niet getrackt. Optioneel verwerkt de app telefoonnummers en technische informatie over de gebruikte systemen (alleen bij aangemelde problemen).

6. Gebruik voor gerechtvaardigde doeleinden

De doeleinden waarvoor de app gegevens verzamelt zijn niet helder geformuleerd in het privacy statement, waardoor geen oordeel over de rechtmatigheid geveld kan worden. Wel geeft Starleaf aan geen persoonsgegevens door te verkopen voor commerciële doeleinden.

7. Passend beschermingsniveau

Het hoofdkantoor Starleaf is gevestigd in London, het Verenigd Koninkrijk, waardoor het momenteel nog direct onder Europese wetgeving valt. Starleaf werkt samen met meerdere sub-verwerkers die zich in de Verenigde Staten bevinden. Hier wordt een deel van de gegevens opgeslagen, waarvoor het bedrijf passende waarborgen heeft getroffen.

3.5 Google Meet

1. Beperking toegang tot de vergadertool en informatie die daarin wordt verwerkt

Google Meet is een tool die steeds meer onderdeel wordt van de Google Suite. Dit is vergelijkbaar met de Office 365 dienstverlening van Microsoft. Dit betekent dat Google Meet gebruik maakt van multi-factor authenticatie. Daarnaast is het mogelijk eigen eisen te stellen aan de sterkte van wachtwoorden die worden gebruikt door medewerkers.

2. Elektronische communicatie beschermen

Google Meet hanteert voor het beschermen van de elektronische communicatie van haar klanten via videovergaderingen dezelfde oplossing als Microsoft Teams. Google Meet maakt gebruik van encryptie voor datastromen die verstuurd worden en data die ‘stil staat’. Google ‘decrypt’ de datastroom zodra het bij haar binnenkomt, om zo haar diensten aan te kunnen bieden.

3. Leverancier is ‘security-minded’ in haar dienstverlening

Naar eigen zeggen verschaft Google zich alleen toegang tot (de data in) vergadersessies vanuit een service-oogpunt. Hier gebruikt Google hetzelfde uitgangspunt als Webex en Teams. Google zegt zelf geen documenten van klanten op te slaan. Net als bij Microsoft zijn opnames van vergadersessies hier een uitzondering, omdat deze wel bij Google in de Cloud worden opgeslagen.
Google Meet heeft als onderdeel van de Google Suite een uitgebreid incident proces. Dit proces voldoet aan vereisten gesteld vanuit de ISO27001 norm.

4. De leverancier voldoet aan relevante security normen

Naast de zojuist genoemde ISO27001 norm, is Google Meet ook ISO27017, ISO27018, SOC 1 en SOC 2 gecertificeerd. De ISO27017 norm is een algemene norm voor security van Cloud providers.

5. Verzameling van minimaal aantal gegevens

De app verzamelt een groot aantal persoonsgegevens van gebruikers. Het generieke privacy statement van alle Google producten benoemt niet specifiek om welke gegevens het gaat voor Google Meet. Een oordeel of sprake is van minimale gegevensverwerking kan dus niet geveld worden.

6. Gebruik voor gerechtvaardigde doeleinden

Google gebruikt verzamelde persoonsgegevens o.a. voor het verbeteren en ontwikkelen van hun (nieuwe) producten, maar maakt niet duidelijk om welke gegevens dit precies gaat en in hoeverre ze wel/niet geanonimiseerd worden. Het bedrijf geeft aan geen persoonsgegevens uit Google Meet te gebruiken om te adverteren of te verkopen aan derde partijen. Wel koppelt Google gegevens uit Google Meet met gegevens uit andere Google producten, waardoor verenigbaar gebruik betwistbaar wordt.

7. Passend beschermingsniveau

Het hoofdkantoor van Google is gevestigd in Californië, de Verenigde Staten, waardoor het niet direct valt onder Europese wetgeving. Het bedrijf beschikt over een Privacy Shield certificering. Gegevensopslag vanuit Google Meet vindt voor Nederlandse gebruikers plaats in Dublin.

4 ADVIES VERSTANDIG GEBRUIK VIDEO VERGADERTOOLS

Naast een analyse van de vijf video vergadertools en advies welke tool HWH zou moeten kiezen op het gebied van security en privacy, heeft HWH VKA ook gevraagd in een advies te voorzien voor verstandig gebruik van dergelijke tools. Dit advies is in dit hoofdstuk verder uitgewerkt en onderverdeeld in verstandig gebruik in het algemeen en verstandig gebruik van de door ons geadviseerde tool: Webex.

4.1.1 Verstandig gebruik algemeen

ORGANISATORISCH

Op organisatorisch gebied is een aantal afspraken voor verstandig gebruik te maken die helpen bij het beschermen van de gegevens die gedeeld worden tijdens video vergaderingen.

Afspraken voor tijdens vergaderen

Maak van tevoren afspraken over wat er wel en niet gedeeld mag worden tijdens online vergaderingen. Denk aan: (bijzondere) persoonsgegevens, vertrouwelijke informatie, bedrijfsdocumenten, etc. Gebruik hiervoor de classificatie van informatie van de organisatie. Neem als uitgangspunt dat er zo min mogelijk gedeeld wordt via de vergadertool.

Als er toch gevoelige informatie gedeeld moet worden, deel dan nooit gevoelige informatie tenzij is vastgesteld dat alle aanwezigen in de vergadering ook daadwerkelijk aanwezig horen te zijn.

Behandel specifiek het opnemen van vergaderingen, indien de gekozen tool dit standaard ondersteunt. Opnames van vergaderingen worden namelijk bijna altijd opgeslagen in de Cloud van de leverancier en zijn in dat geval ook voor hen toegankelijk.

Omgang

Zorg dat medewerkers elkaar (kunnen) aanspreken op onverstandig gebruik. Maak dit bespreekbaar door dit aan te kaarten in bijvoorbeeld een intern nieuwsbericht of in vergaderingen van de teams.

TECHNISCH

Op technisch gebied is er in het algemeen al een aantal maatregelen denkbaar voor het verstandig gebruik van video vergadertools, die op alle tools toepasbaar zijn.

Security- en Privacy vriendelijke technische mogelijkheden

Maak binnen de organisatie duidelijk welke security- en privacy vriendelijke functionaliteiten een tool aanbiedt (bijvoorbeeld autorisatie-instellingen of mogelijkheden om minder gegevens te delen) en zet deze zoveel mogelijk standaard aan.

'Expert'-gebruikers aanstellen

Stel binnen de organisatie in elke afdeling medewerkers aan die 'expert'-gebruiker worden. Deze gebruikers worden specifiek op het gebied van security en privacy ingelicht over de mogelijkheden van de tool en vereisten vanuit de organisatie en kunnen als vraagbaak dienen voor de afdeling.

4.1.2 Verstandig gebruik Webex

Webex biedt voor hosts een groot aantal mogelijkheden tot verstandig gebruik van de tool. Afhankelijk van de voorkeuren van de organisatie is veel in te stellen of aan te passen. Wij adviseren bij het gebruik van Webex in ieder geval de volgende maatregelen te nemen:

Algemeen

- Deel je Audio PIN met niemand
- Deel wachtwoorden voor vergaderingen alleen met mensen die daadwerkelijk toegang nodig hebben tot de vergadering

Inplannen vergaderingen

- Maak de afweging of de vergadering op de algemene vergadering-agenda (meeting calender) zichtbaar moet zijn. Het is mogelijk dit niet te doen.
- Als de vergadering hier toch zichtbaar moet zijn, kies dan een naam voor de vergadering die geen gevoelige informatie over de inhoud van de vergadering prijsgeeft (voorkom bijvoorbeeld een dergelijke naam: bespreken ontslag collega X)
- Bepaal van tevoren het niveau van security die de vergadering nodig heeft. Gevoelige vergaderingen kunnen naast bescherming met een wachtwoord ook onzichtbaar worden gemaakt voor een ieder die niet is uitgenodigd.
- Gebruik een complex wachtwoord voor toegang tot de vergadering. Sluit hierbij aan op de wachtwoordvereisten van HWH. Gebruik een wachtwoord niet meerdere keren.
- Het is mogelijk het wachtwoord voor de vergadering niet bij te voegen in de uitnodigingsmail voor een vergadering. Vooral voor vergaderingen met meer gevoelige onderwerpen is het aan te raden het wachtwoord niet mee te zenden, maar via bijvoorbeeld een SMS apart te verzenden naar de genodigden.
- Maak een afweging of genodigden mogen toetreden voordat de host de vergadering heeft gestart. Als dat wel toegestaan is, beperk dan de autorisaties die de genodigden hebben tijdens afwezigheid van de host.
- Stel van tevoren een alternatieve host aan voor vergaderingen waar gevoelige informatie wordt gedeeld. Dit voorkomt dat bij het wegvallen van de originele host de ‘hosting-rechten’ naar een genodigde gaan die deze rechten niet zou moeten hebben.

Tijdens de vergadering

- Beperk de toegang tot de vergadering wanneer alle genodigden aanwezig zijn. Dit kan indien nodig tijdens de vergadering ook tijdelijk opgeheven worden.
- Deel als het mogelijk is niet volledige schermen tijdens de vergadering, maar alleen vensters van applicaties.

Na de vergadering

- Indien er opnames van de vergadering zijn gemaakt, bescherm deze dan met een wachtwoord.
- Wanneer de opname niet meer bewaard hoeft te worden, verwijder deze dan.

A Bijlage A - bronnen

ZOOM

1. https://zoom.us/security

2. https://dev.io/posts/zoomzoo/ ; https://advisories.ncsc.nl/advisory?id=NCSC-2020-0308&version=1.00&format=plain

3. https://www.nu.nl/tech/6040727/videobel-app-zoom-stuurt-stiekem-gebruikersdata-naar-facebook.html

4. https://zoom.us/privacy

5. https://www.bright.nl/nieuws/artikel/5074221/videobel-app-zoom-stopt-stiekeme-datadeling-met-facebook

6. https://blog.zoom.us/wordpress/2020/04/20/data-routing-control-is-here/

7. https://www.bright.nl/nieuws/artikel/5090086/zoom-laat-betalende-gebruikers-regio-van-server-kiezen

8. https://www.bitsoffreedom.nl/2020/04/07/wegwijs-in-de-tools-om-te-videobellen/

WEBEX

9. https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html#CiscoWebexDataCenterSecurity

10. https://www.cisco.com/c/en/us/about/legal/privacy-full.html

11. https://article.images.consumerreports.org/prod/content/dam/CRO-Images-2020/Electronics/Cisco_Webex_Meetings_Privacy_Data_Sheet

12. https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts

MS TEAMS

13. https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview

14. https://privacy.microsoft.com/nl-nl/privacystatement

15. https://www.microsoft.com/nl-nl/trust-center/privacy?market=nl

16. https://medium.com/cr-digital-lab/skype-teams-microsoft-policy-review-299bd1403c4b

STARLEAF

17. https://support.starleaf.com/legal-information/starleaf-privacy-notice/

18. https://www.starleaf.com/assets/Uploads/starleaf-security-white-paper-2018-1.pdf

GOOGLE MEET

19. https://cloud.google.com/blog/products/g-suite/how-google-meet-keeps-video-conferences-secure

20. https://support.google.com/a/answer/7582940?hl=en

21. https://cloud.google.com/security/privacy

22. https://support.google.com/a/answer/7582940?hl=nl