Grant Thornton

Videoconferencing tools

Een leidraad naar een veilige keuze

Samenvatting

Nu veel mensen door het coronavirus thuiswerken, zijn videobellen en -conferencen bijna onmisbaar voor de samenwerking. Maar hoe maak je als mkb-ondernemer nu een goede keuze uit het aanbod van verschillende videoconferencing tools? Wat zijn belangrijke zaken waar je op moet letten? En hoe weet je of de informatie die gedeeld wordt via deze programma's veilig is en blijft?

In dit rapport geven we u inzicht in de 10 meest voorkomende thuiswerkoplossingen (inclusief videobellen) die wij tegenkomen in het veld bij onze relaties. Iedere videoconferencing tool is aan de hand van deskresearch, beoordeeld op 5 punten. Dit zijn 5 belangrijke punten waar onze relaties hun videoconferencing tools onder andere op beoordelen:

- Welke functionaliteiten kent de oplossing?
- Hoe zit het met de gegevensopslag (welke privacygevoelige data slaat de tool op)?
- Hoe verlopen de informatiestromen?
- Hoe staat het met de beveiliging?
- Welk betaalmodel hanteert de tool?

De 10 thuiswerkoplossingen die we hebben onderzocht, zijn: Microsoft Teams, Lifesize, Google Meet, Zoom, Jitsi, Cisco WebEx, Slack, GoToMeeting, Signal en Skype for Business.

Natuurlijk kunnen we dit rapport uitbreiden met nog meer oplossingen of dieper in gaan op iedere specifieke oplossing, echter het doel van deze leidraad is om op hoofdlijnen inzicht te verschaffen in de veiligheid van de tools, en geen advies te geven over wat de beste tool is. Immers een dergelijk advies is geheel afhankelijk van de individuele wensen van uw onderneming en uw medewerkers.

Wel geven wij een aantal tips mee om het risico op inbreuk op privacy te beperken en de veiligheid van het gebruik van dergelijke oplossingen te vergroten.

1. Dwing het gebruik van sterke wachtwoorden af vanuit uw systemen en toepassingen.
2. Maak gebruik van Multi-Factor Authenticatie.
3. Sla bedrijfsgevoelige informatie op in een sterk beveiligde omgeving.

Wanneer je als mkb-ondernemer overgaat tot een uiteindelijke pakketselectie is het van belang om uitgebreider te kijken naar functionaliteiten en gebruiksgemak van de tool. Wij hebben ons beperkt tot de bovenstaande 5 onderdelen die zich in grotere mate richten op de veiligheid van de tools.

Overzicht videoconferencing tools

Hoe scoren de 10 videoconferencing tools op de 5 verschillende aspecten? Hieronder een overzicht. Voor meer informatie over de applicaties kunt u klikken op de links onderaan de pagina.

Wat biedt de app?	Teams	Lifesize	Google Meet	Zoom	Jitsi	Cisco WebEx	Slack	GoTo-meeting	Signal	Skype for business
(Groeps)chat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1-op-1 gesprekken (audio/video)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Groepsgesprekken (audio/video)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zelf opzetten en beheren	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓
Deelname zonder account	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗
Gebruik in browser	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓
Gebruik op verschillende platformen	✓	✓	✓	✓[2]	✓	✓	✓	✓	✓	✓
Maximaal aantal deelnemers per gesprek	250	1000	250	500	25	1000	15	250+	2	1000
Wat slaat de app op?										
Locatie gegevens	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓
Gespreksgegevens	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓
Metadata (gegevens over de gesprekken)	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓
Hoe verloopt de informatiestroom										
Verwerkersovereenkomst mogelijk	✓	✓	✓	✓	n.v.t.	✓	✓	✓	✗	✓
Verstrekking van gegevens aan derde partijen	✓[1]	✓[1]	✓[1]	✗	n.v.t.	✓[1]	✓[1]	✓[1]	✗	✓[1]
Locatie verwerkings-verantwoordelijke	VS	VS	VS	VS	n.v.t.	VS	VS	VS	VS	VS
Gegevens blijven binnen Nederland/EU	✓	✗	✓	✓	n.v.t.	✓[4]	✓[4]	✗	✗	✓
Zijn de gegevens beveiligd?										
End-to-end versleuteling (aanbieder kan niet bij inhoud)	✗	✗	✗	Zomer 2020	✓[3]	✓[5]	✗	✓	✓	✗
Versleuteling van verkeer onderweg (aanbieder kan wel bij inhoud, derden niet)	✓	✓	✓	✓	✓[3]	✓[5]	✓	✗	✗	✓
Iedereen kan de broncode controleren (open source)	✗	✗	✗	✗	✓[3]	✗	✗	✗	✓	✗
Model van afname?										
Abonnement	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓
Gratis versie/demo	✓	✓	✓	✓	✓	✓	✓[6]	✓	✓	✗
Extra informatie										

1 Indien hier noodzaak voor is vanuit een juridisch perspectief
2 Is enkel te gebruiken in een browser
3 Is afhankelijk van hoe het op de eigen server is ingesteld
4 Is mogelijk bij de duurdere abonnementsvormen
5 Bij de gratis dienst is geen zekerheid over de locatie
6 Bij de gratis versie is geen videobellen inbegrepen

Let op! Grant Thornton heeft geen uitgebreid technisch onderzoek verricht naar bovenstaande applicaties. Alle informatie is gebaseerd op wat de bedrijven zelf in hun privacy verklaringen hebben vermeldt, dan wel van betrouwbare bronnen.


Isabella
Available
Home
New
Contacts
Isabella, Emily K, Anthony
Emily K.
Matthew D.
Anthony
Adrew
Jayden CK.
Ava
Matthew D.
Emily K.

Hoe veilig is Microsoft Teams?

Een van de meest gebruikte tools voor videovergaderen is op dit moment Microsoft Teams. Deze applicatie, die Skype for Business gaat vervangen, is standaard bij een Microsoft 365 abonnement. Hoe zit het met de privacy en beveiliging van deze oplossing en wat kan het?

Wat belooft het?

Teams belooft een oplossing te bieden waarbij iedereen binnen een team, afdeling en/of onderneming vanuit één applicatie kan werken, vergaderen, onderling bellen met maximaal 250 deelnemers en chatten, onafhankelijk waar de gebruiker zich fysiek bevindt. Teams onderscheidt zich in het bieden van integratie met andere Microsoft toepassingen zoals Sharepoint en Exchange, Yammer en Onedrive.

Manier van inloggen?

Teams maakt gebruik van de koppeling met Microsoft 365. Dat wil zeggen dat als er al ingelogd is met het Microsoft account er automatisch wordt ingelogd bij Teams (Single Sign-On). Wanneer niet is ingelogd met een bestaand Microsoft 365 account, worden de inloggegevens en eventuele Multi-Factor Authentication gebruikt van het Microsoft account. Dit biedt de mogelijkheid om over de hele Microsoft omgeving dezelfde vereisten voor de beveiliging in te stellen. Het is ook mogelijk om een gastaccount te maken voor een vergadering. Voorwaarde is wel dat de organisator over een Microsoft account beschikt.

Wat wordt van mij opgeslagen en hoe?

Teams slaat redelijk wat gegevens op. Zo verzamelt Teams uw NAW gegevens, demografische gegevens, apparaat en verbruiksgegevens, uw zoekacties en opdrachten, spraakgegevens en locatiegegevens om maar een greep uit het assortiment te doen. Dit geldt overigens voor alle Microsoft applicaties en diensten. Hierbij komt dat alleen gebruik wordt gemaakt van versleuteling tussen de server en de gebruiker en niet end-to-end.

Microsoft heeft dus de mogelijkheid om data in te zien. Volgens Microsoft wordt de data uitsluitend gebruikt om de diensten te verbeteren.

En de AVG dan?

Microsoft is AVG-proof, in de zin dat data binnen de EU wordt opgeslagen. Ze hebben een privacy verklaring en verstrekken beperkt gegevens aan derde partijen (enkel de overheid als hier vanuit een wettelijk perspectief noodzaak voor is). De locatie van de data is inzichtelijk voor de group controller. Het is ook mogelijk om de data van Teams op een eigen server op te slaan.

Ik heb een aanbod gekregen, maar voor wat?

Op dit moment biedt Microsoft gratis licenties aan de ondernemingen die een Microsoft verkoopconsultant hebben. Net zoals met alle Microsoft abonnementen zit Teams hier ook standaard bij. Echter, betreft dit een E1 type licentie. Dit is de meest basale vorm van een Microsoft Office 365 abonnement en biedt dan ook veel minder tools met betrekking tot security en privacy ten opzichte van de andere licenties.

Er is geen eenduidig antwoord te geven op de veiligheid van Teams. Dit is sterk afhankelijk van de configuratie van de hele Microsoft Office 365 omgeving. Het kan dus zo sterk en zwak beveiligd zijn als uw onderneming heeft ingesteld. Indien aan de volgende eisen wordt voldaan, kan Teams veilig worden genoemd:

- Maak gebruik van een sterk wachtwoord en Multi-Factor Authentication.
- Sla communicaties waarin bedrijfsgevoelige informatie besproken wordt op in een extra beveiligde omgeving.

Hoe veilig is Lifesize?

Lifesize is een in Nederland relatief onbekende applicatie voor videovergaderingen. Deze onderneming uit de Verenigde Staten onderscheidt zich door potentieel 4k videobellen aan te bieden. Hoe zit het met de beveiliging en privacyaspecten van deze oplossing?

Wat belooft het?

Lifesize belooft de mogelijkheid om in 4k kwaliteit vergaderingen te houden, deelname tot 1000 deelnemers, een chatfunctie en bestandsdeling. Voor de klanten in de US bieden zij ook audiobellen aan.

Manier van inloggen?

Lifesize biedt de mogelijkheid gebruikersaccounts aan te maken in de applicatie zelf. Standaard wordt gebruik gemaakt van een gebruikersnaam (e-mailadres) en wachtwoord. In dat geval worden de accountgegevens door Lifesize opgeslagen. Het is mogelijk om een koppeling te maken met Lifesize doormiddel van een programma van derden om zo direct ingelogd te zijn (Single Sign-on). Deze moet eerst nog aangeschaft en geïnstalleerd worden. Zo kan er ook gebruik gemaakt worden van Multi-Factor Authentication.

Wat wordt van mij opgeslagen en hoe?

Lifesize verzamelt accountgegevens, gebruiksgegevens en technische ondersteuningsgegevens (30 dagen). In het Data Processing Addendum wordt ruimte gegeven voor het verwerken van meer dan de hiervoor genoemde gegevens. Er kan een verwerkingsovereenkomst getekend worden. Hierbij komt dat er alleen gebruik wordt gemaakt van versleuteling tussen de server en de gebruiker en niet end-to-end. Lifesize heeft dus de mogelijkheid om data in te zien.

En de AVG dan?

Lifesize is compliant aan de AVG doormiddel van de EU-US Privacy Shield Frameworks. Dit is erkend door de EU en voldoet daardoor aan de AVG, ondanks dat de gegevens niet binnen de EU blijven. In tegenstelling tot bijvoorbeeld Teams is het voor Lifesize gebruikers niet inzichtelijk in welk datacentrum hun data is opgeslagen.

Is de gratis versie voor mij?

Bij de gratis versie van Lifesize is het vergaderen tot 25 personen in een eigen meeting room door middel van de desktop of mobiele applicatie inbegrepen. Lifesize biedt ook betaalde abonnementen waarbij tot 1000 mensen tegelijk aan dezelfde vergadering kunnen deelnemen.
Daarnaast bieden de Plus en Enterprise versie ook integraties met Microsoft 365 en de mogelijkheid om vergaderingen op te nemen. Het is dus zeer afhankelijk van uw wensen en benodigdheden welke vorm van Lifesize het beste bij u past.

Uit dit korte onderzoek blijkt dat Lifesize zich heeft ingespannen om zowel op privacy- als op securitygebied zeer betrouwbaar te zijn en toch een gebruikersvriendelijk platform te bieden. Met de volgende 2 aanbevelingen is de veiligheid van gebruik van Lifesize dus te waarborgen:

- Gebruik Single sign-on en Multi-Factor Authentication met een eigen dienst of programma.
- Sla communicaties waarin bedrijfsgevoelige informatie besproken wordt op in een extra beveiligde omgeving.

Hoe veilig is Google Meet?

Een dienst die werkt binnen een webbrowser, waardoor geen app geïnstalleerd hoeft te worden. Het maakt gebruik van accounts die al aanwezig zijn, als in de organisatie gebruik gemaakt wordt van diensten uit de G Suite. Maar hoe zit het met hun beveiliging en privacy aspecten van deze oplossing?

Wat belooft het?

Google Meet is een dienst binnen de G Suite van Google. Het biedt videovergaderen voor maximaal 250 deelnemers tegelijk, met diverse security- en privacyfuncties.
Google Meet werkt binnen een webbrowser, waardoor het op vrijwel elk apparaat met een browser werkt, zonder dat een app geïnstalleerd hoeft te worden.

Manier van inloggen?

Omdat Google Meet binnen de G Suite van Google valt, maakt het gebruik van Google accounts, zoals die ook gebruikt worden voor bijvoorbeeld Gmail en Google Docs. Hierdoor kunt u gebruikmaken van Multi-Factor Authenticatie via bijvoorbeeld Google Authenticator of SMS-berichten. Het deelnemen aan de vergadering gaat door het benaderen van de vergadering-ID, die verstrekt wordt door de organisator. De vergaderingen kunnen beveiligd worden met een PIN. Dit is een extra beveiliging, waardoor ook het raden van een vergadering-ID geen toegang biedt.

Wat wordt van mij opgeslagen en hoe?

De oplossing maakt gebruik van Google accounts. Alle gegevens over deze accounts worden opgeslagen in de Google Cloud. Google Cloud heeft een privacy policy en de mogelijkheid een verwerkersovereenkomst af te sluiten. Google heeft aangetoond GDPR compliant te zijn. Daarbij moet in gedachten gehouden worden dat het verdienmodel van Google het verkopen van data is. Google doet geen inspanning het gebruik van metadata te minimaliseren. Audio, video, chat en documenten van de vergaderingen worden opgeslagen in Google Cloud. Daarbij wordt zowel tijdens transport als bij opslag encryptie gebruikt. Google Meet biedt geen mogelijkheid een eigen server te gebruiken.

En de AVG dan?

Google Meet is nauw verweven met Google Cloud, waar alle gegevens opgeslagen worden. Google Cloud heeft een uitgebreide privacy policy. Het biedt de mogelijkheid een verwerkersovereenkomst af te sluiten.
U hebt altijd inzicht in waar uw gegevens opgeslagen zijn. Voor Europese gebruikers is dat altijd binnen de EU. Het is niet een bekend waar de gegevens worden opgeslagen als een organisator buiten de EU de vergadering opslaat.

Ik heb een aanbod gekregen, maar voor wat?

Licenties zijn gratis voor persoonlijk gebruik. De meest gebruikte licenties binnen ondernemingen zijn de G Suite licenties. Google biedt de G Suite Essentials tot en met 30 september 2020 gratis aan. Daarmee kunt u gebruikmaken van 50 extra deelnemers (150 in plaats van 100), internationale inbelnummers en een hogere opslaglimiet (100GB in plaats van 15GB). De G Suite Enterprise Essentials biedt 250 deelnemers en nog meer functionaliteiten, maar is niet gratis.

Google Meet behandelt uw gegevens zorgvuldig door encryptie te gebruiken tijdens het transport en bij opslag in Google Cloud. Het geeft inzicht in welke gegevens waar opgeslagen worden en heeft aangetoond aan de GDPR te voldoen. Waar Google in het verleden negatief in het nieuws geweest is vanwege het oneigenlijk verzamelen van persoonlijke gegevens, lijkt dat bij deze dienst wel in orde te zijn. Neem wel de volgende adviezen in overweging:

- Beveilig de vergaderingen altijd met een PIN.
- Sla video's waarin bedrijfskritische informatie wordt besproken liever niet op.

Hoe veilig is Zoom?

Zoom zegt de meest gebruikersvriendelijke oplossing te zijn met alle functionaliteiten die u zich maar kunt wensen. Hoe zit het met de beveiligings- en privacy-aspecten van deze oplossing?

Wat belooft het?

Zoom belooft vooral gebruiksgemak. De tool werkt op vrijwel alle platformen, zelfs inclusief hardware van concurrenten. Zoom is hard bezig de beveiliging van de oplossing te verbeteren en het heeft al een aantal functionaliteiten die andere oplossingen niet bieden, vooral gericht op het beschermen van bedrijfsinformatie, zoals het watermerken van opnames. Verder biedt het ook de gebruikelijke functionaliteiten zoals het beveiligen van vergaderingen en diverse functionaliteiten om deelnemers te controleren.

Manier van inloggen?

Elke organisator van een vergadering heeft een Zoom-account nodig. Zoom ondersteunt Single Sign-On en Multi-Factor Authenticatie. Deelnemers hebben geen account nodig, alleen een e-mailadres. Er zijn apps beschikbaar voor vrijwel alle platforms, maar het is ook mogelijk de webversie te gebruiken zonder een app te installeren.

Wat wordt van mij opgeslagen en hoe?

De app verzamelt accountgegevens, locatiegegevens, gebruiksgegevens en technische ondersteuningsgegevens. In het Data Processing Addendum wordt ruimte gegeven voor het verwerken van meer dan de hiervoor genoemde gegevens. Er kan een verwerkersovereenkomst afgesloten worden.

En de AVG dan?

Zoom is compliant aan de AVG doormiddel van de EU-US Privacy Shield Frameworks. Dit is erkend door de EU en voldoet daardoor aan de AVG, ondanks dat de gegevens niet binnen de EU blijven. Zoom biedt ook de mogelijkheid om per regio aan te geven of de gegevens daar verwerkt mogen worden of niet. Het is daarmee mogelijk om ervoor te zorgen dat de data uitsluitend binnen de EU blijft.

Zoom in het nieuws

Waarschijnlijk kent u Zoom uit het nieuws, waarin gerapporteerd werd dat de onderneming al uw gegevens op straat had laten belanden. Het spreekt voor zich, dat dit een enorme imagoschade heeft opgeleverd voor Zoom. Gelukkig heeft het er ook voor gezorgd dat Zoom de tekortkomingen met man en macht aan het oplossen is. De oplossing is daarom ook nu nog volop in ontwikkeling en er worden nog steeds beveiligingsfunctionalteiten toegevoegd. Een belangrijke functionaliteit, die op de planning staat, is end-to-end encryptie, dit zorgt ervoor dat Zoom uw vergaderingen niet meer kan inzien.

De negatieve berichtgeving over Zoom heeft ervoor gezorgd dat de tekortkomingen snel worden opgelost. Versie 5.0 van de app is nu beschikbaar en alle gebruikers hebben deze versie uiterlijk 30 mei 2020 in gebruik moeten nemen. De tip die meegegeven wordt is:

- Maak altijd gebruik van de aangeboden beveiligingsfunctionaliteiten om uw vergaderingen te beveiligen.

Hoe veilig is Jitsi?

Jitsi is een open source project dat voor iedereen gratis te gebruiken is. Het is ontworpen om het hoogst mogelijke niveau van privacy en security te bieden. Dus hoe zit het met de beveiliging en privacy aspecten van deze oplossing?

Wat belooft het?

Jitsi belooft een videoconferencing tool die uw privacy en security waarborgt. Jitsi is gratis te gebruiken en biedt toch veel functionaliteiten die bij andere aanbieders geld kosten.

Manier van inloggen?

Jitsi Maakt geen gebruik van accounts of van inloggen. Direct vanaf de website Jitsi.org kunt u een videoconferentie opzetten. De link naar deze conferentie en de bijbehorende PIN kunt u op elke manier die u maar wenst delen met uw deelnemers. U kunt ook een eigen server opzetten en dan ook uw video opslaan (zonder eigen server kan dat niet). De software en ondersteuning zijn daarvoor gratis te verkrijgen op Jitsi.org. Daar kunt u ook de broncode inzien. In tegenstelling tot veel andere platformen maakt Jitsi dit openbaar. Met een eigen server bent u ervan verzekerd dat er geen gegevens gedeeld worden met of opgeslagen worden door Jitsi. Bij het onderhouden van een eigen server hebt u natuurlijk wel zelf de technische kennis en capaciteit nodig.

Wat wordt van mij opgeslagen en hoe?

Jitsi verzamelt geen gegevens. U hoeft niet in te loggen om een vergadering te starten. Deelnemers hebben slechts een link naar de vergadering en het bijbehorende password nodig. Helemaal bij het gebruik van een eigen server is volledig uit te sluiten dat Jitsi toegang tot gegevens krijgt. Jitsi maakt gebruik van end-to-end encryptie, wat ervoor zorgt dat ongeautoriseerde personen de vergaderingen op geen enkel moment kunnen inzien.

En de AVG dan?

Jitsi verzamelt geen persoonsgegevens en heeft daarom geen verplichtingen aangaande de AVG.

Is de gratis versie voor mij?

Jitsi biedt alleen een gratis versie aan. Jitsi toont geen advertenties, verkoopt geen gegevens en accepteert geen donaties. Het project is open source freeware en wordt volledig financieel gedragen door het bedrijf 8×8. Met de gratis software is een eigen server op te zetten en met diverse modules (projecten) helemaal aan te passen naar eigen wensen. De oplossing moet dan natuurlijk wel zelf beheerd en onderhouden worden.

Jitsi is dé oplossing om te gebruiken wanneer privacy en het beschermen van bedrijfsgegevens voorop staat. Met end-to-end encryptie en de aanmoediging een eigen server op te zetten, is Jitsi de best beveiligde oplossing die te krijgen is. Als uw onderneming de kennis en capaciteit heeft om de oplossing zelf te hosten, verdient deze gratis oplossing, die erg goed aan eigen wensen is aan te passen, zeker de aanbeveling. Onthoud in ieder geval de volgende tips voor een veilige omgeving:

- Gebruik de PIN functionaliteit voor al uw vergaderingen.
- Pas sterke wachtwoorden toe voor de vergaderingen.
- Sla bedrijfsgevoelige informatie op in een sterk beveiligde omgeving.

Hoe veilig is Cisco WebEx?

Cisco WebEx is een videoconferencing oplossing van de grote speler op de IT-markt: Cisco. Dit bedrijf, met een goede reputatie, heeft de oplossing Cisco WebEx in haar aanbod van diensten. Hoe zit het met de veiligheid van deze oplossing?

Wat belooft het?

Cisco WebEx belooft vooral een gemakkelijk te gebruiken oplossing te zijn. Het biedt functionaliteiten die niet veel verschilen van andere oplossingen. Cisco WebEx belooft de mogelijkheid tot 1000 deelnemers per vergadering.

Manier van inloggen?

Voor het inloggen als organisator van een vergadering is een WebEx account nodig. Het account is gekoppeld aan een licentie. Voor het deelnemen aan een vergadering is geen account nodig. WebEx ondersteunt zelf geen Single Sign-on of Multi-Factor Authenticatie, maar er kan gebruikt gemaakt worden van een eigen Identity Provider die deze zaken wel ondersteunt.

Wat wordt van mij opgeslagen en hoe?

Cisco WebEx verzamelt behoorlijk wat gegevens, zoals naam, locatie, telefoon, gegevens over het gebruikte device, IP-Adres, tot zelfs gebruikersinformatie uit Active Directory, als die aangesloten is. Van de host van een vergadering wordt nog meer verzameld, zoals vergadergegevens, waaronder zelfs de opgenomen vergadering, documenten en transcripts. De gebruiker kan te allen tijde de verzamelde gegevens inzien.

En de AVG dan?

Cisco WebEx is naar eigen zeggen compliant aan de AVG door middel van de EU-US Privacy Shield Frameworks. Dit is erkend door de EU en voldoet daardoor ondanks dat de gegevens niet binnen de EU blijven, toch aan de AVG. Wanneer we echter kijken naar de aard en hoeveelheid gegevens die verzameld worden, zijn die niet allemaal te vatten in de genoemde grondslagen.

Waar blijft mijn data?

Voor de betaalde dienst wordt data die door gebruikers gegenereerd wordt (zoals opnames van vergaderingen en hun metadata) opgeslagen in een datacentrum in de regio van de gebruiker. Voor Nederland is dat het datacentrum in Amsterdam. Voor de gratis dienst kunnen de gegevens ook elders opgeslagen worden. De facturatie informatie en analyse data worden altijd opgeslagen in de Verenigde Staten.

Cisco WebEx is een videoconferencing tool van een grote marktspeler met een goede reputatie. Ze adverteren vooral met gebruiksgemak en niet zozeer met uitgebreide functionaliteiten. WebEx zegt optioneel end-to-end encryptie aan te bieden, maar dat wordt in geen van de abonnementsvormen expliciet genoemd. WebEx verzamelt erg veel gegevens en lang niet altijd goed onderbouwd met een grondslag. Hanteer de volgende voorwaarden om veilig gebruik te kunnen maken van Cisco WebEx:

- Gebruik sterke wachtwoorden voor alle accounts.
- Sla bedrijfsgevoelige informatie op in een sterk beveiligde omgeving.

Hoe veilig is Slack?

Slack is een collaboratiesuite waarvan videoconferencing maar een klein onderdeel is. Het is vooral gericht op gebruik in wat kleinere organisaties, aangezien de videoconferencing maximaal 15 deelnemers toestaat. Hoe zit het met de beveiliging en privacy aspecten van deze oplossing?

Wat belooft het?

Slack is in eerste instantie een samenwerkingsplatform voor teams, met de nadruk op bestandsdeling en planning. Videobellen met maximaal 15 deelnemers is een extra functie. In die zin heeft het de omgekeerde benadering van de meeste andere videoconferencing tools.
Het videobellen in Slack is dan ook niet heel erg uitgebreid.

Manier van inloggen?

Inloggen gaat met een Slack account, of door een integratie met de eigen Identity Provider van de organisatie.
Single Sign-on en Multi-Factor Authenticatie worden op die manier ondersteund.

Wat wordt van mij opgeslagen en hoe?

De app verzamelt accountgegevens als e-mailadres, telefoon, account en password.
Ook verzamelt het gebruiksgegevens als metadata, log data, locatiedata en apparaat gegevens.
De verzamelde gegevens zijn voor de gebruiker in te zien.

En de AVG dan?

Slack slaat gegevens standaard op in de Verenigde Staten, maar in de twee hoogste betaalde versies krijgt men de optie Data Residency. Daarmee kan gekozen worden waar de gegevens opgeslagen moeten worden.

Er zijn meerdere mogelijkheden om daarvoor een locatie binnen de EU te kiezen. Sinds 1 januari 2020 is Slack ook gecertificeerd volgens het EU-US en Swiss-US Privacy Shield en daarmee voldoet het aan de AVG. Er is een Data Processing Addendum dat getekend kan worden door de onderneming en daarmee een verwerkersovereenkomst vaststelt.

Is de gratis versie voor mij?

Videobellen is niet aanwezig in de gratis versie.
Er zijn 3 niveaus van de betaalde versie. In alle 3 die niveaus zijn de functionaliteiten voor het videobellen gelijk: maximaal 15 deelnemers en geen opslag van opgenomen videogesprekken.

Het is duidelijk dat videobellen niet de belangrijkste functie is van Slack. Het ontbreken van opslag van opgenomen vergaderingen zorgt in elk geval voor een verminderd risico. Verder wordt alle data op het platform versleuteld in transit en at rest. De hoogste 2 licentieniveaus geven meer controle over de locatie van de opgeslagen data en verdienen dan ook de aanbeveling. Met de volgende tips bent u goed op weg naar het veilig gebruiken van Slack:

- Gebruik een sterk wachtwoord en maakt gebruik van Multi-Factor Authenticatie.
- Sla bedrijfsgevoelige informatie op in een sterk beveiligde omgeving.

Hoe veilig is GoToMeeting?

Een oplossing om vanuit huis te vergaderen, is GoToMeeting. De toepassing van moederbedrijf LogMeIn, onderdeel van de remote desktop applicatie Citrix, biedt HD videobellen, presenteren, online seminars tot 3000 deelnemers en een 'Call me' functie.

Wat belooft het?

GoToMeeting belooft een eenvoudige oplossing te zijn voor videobellen en vergaderen. Ook bieden zij apparatuur voor vergaderruimtes aan om de meest optimale ervaring te garanderen. Met de 'Call me' functie kunnen deelnemers worden gebeld op het telefoonnummer dat is ingevoerd wanneer de vergadering begint. Dit is zeker geschikt voor ondernemingen met werknemers die veel onderweg zijn en niet altijd beschikking hebben tot stabiel internet. Daarnaast biedt GoToMeeting meer specifieke functies om de visuele aantrekkelijkheid van de organisator te vergroten.

Manier van inloggen?

GoToMeeting kan gebruikmaken van een koppeling met de Active Directory. Dat wil zeggen, dat als er al ingelogd is op de desktopomgeving, er automatisch wordt ingelogd bij GoToMeeting (Single Sign-On). Afhankelijk van de Active Directory instellingen is Multi-Factor Authentication mogelijk. Het is mogelijk om een gastaccount te maken voor een vergadering. Voorwaarde is wel dat de organisator over een GoToMeeting-account beschikt.

Wat wordt van mij opgeslagen en hoe?

GoToMeeting verzamelt redelijk wat gegevens zoals: NAW-gegevens, demografische gegevens, apparaat- en verbruiksgegevens, functie binnen de onderneming en locatiegegevens. Wel maakt GoToMeeting gebruik van end-to-end encryptie. Dit houdt in dat GoToMeeting niet de exacte inhoud van de communicatie kan inzien. De data wordt volgens GoToMeeting gebruikt om de diensten te verbeteren en gerichte aanbiedingen te doen van haar eigen producten.

En de AVG dan?

GoToMeeting is compliant aan de AVG door middel van de EU-US Privacy Shield Frameworks. Dit is erkend door de EU en voldoet daardoor, ondanks dat de gegevens niet binnen de EU blijven, toch aan de AVG. In tegenstelling tot bijvoorbeeld Teams kunnen GoToMeeting gebruikers niet inzien in welk datacentrum hun data is opgeslagen.

Welke versie moet ik nemen?

GoToMeeting biedt 3 'pakketten' aan en een tijdelijke gratis versie. Welke versie geschikt is voor u, is sterk afhankelijk van het aantal deelnemers in een vergadering. Tot 150 deelnemers is het 'Professional abonnement' geschikt, tussen de 150 en 250 deelnemers is er het 'Business plan' en daarboven wordt verzocht om contact op te nemen met GoToMeeting voor een op maat gemaakt 'Enterprise plan'. Vanaf het Business plan zijn er aanvullende functies, welke voornamelijk gaan over het opnemen en opslaan van video's en momentopnames in de Cloud. Bij het Enterprise plan zijn trainingen voor werknemers ook inbegrepen.

Uit dit korte onderzoek blijkt dat GoToMeeting zich heeft ingespannen om zowel op privacy- als op security gebied zeer betrouwbaar te zijn en toch een gebruiksvriendelijk platform te bieden. Met de volgende 2 aanbevelingen is het gebruik van GoToMeeting dus veilig te noemen:

- Gebruik Single Sign-On en Multi-Factor Authentication met een eigen dienst of programma.
- Sla communicaties waarin bedrijfsgevoelige informatie besproken wordt op in een extra beveiligde omgeving.

Hoe veilig is Signal?

Signal is een non-profit-aanbieder van videobellen en -vergaderen en chatten. Signal focust vooral op privacy. Signal is een gratis platform wat net zoals Whatsapp gebruik maakt van een telefoonnummer voor de identificatie van een gebruiker. Voor het gebruik van de desktopversie is dus de smartphone app verplicht.

Wat belooft het?

Signal belooft eenvoudig gebruik, HD kwaliteit videobellen en de optimale privacy voor een communicatie applicatie. Qua layout en gebruiksgemak is het zeer te vergelijken met Whatsapp.

Manier van inloggen?

Signal maakt gebruik van dezelfde manier van inloggen als Whatsapp, door middel van een SMS-verificatie op het opgegeven telefoonnummer. Vervolgens kan door middel van een QR-code verbinding gemaakt worden met de desktop variant van de applicatie.
In tegenstelling tot Whatsapp wordt een pincode gevraagd aan de gebruiker wanneer deze voor de eerste keer inlogt. Deze pincode moet elke keer dat er gebruik wordt gemaakt van een nieuwe mobiele telefoon ingevoerd worden. Zonder mobiel nummer kan er dus geen gebruik worden gemaakt van Signal. Daarbij kan ingesteld worden dat elke keer dat het scherm wordt vergrendeld, Signal ook wordt vergrendeld en ontgrendeld kan worden doormiddel van biometrics (vingerafdruk, et cetera).

Wat wordt van mij opgeslagen en hoe?

Signal verplicht toegang tot een telefoonnummer, bestanden op de mobiele telefoon, toegang tot het maken van oproepen en contactpersonen. Signal doet dit zodat zij haar diensten aan kan bieden. Daarnaast worden de gegevens van de contactpersonen voor een natuurlijk persoon onherkenbaar gemaakt en vervolgens gematched met de database van Signal, zodat contact suggesties kunnen worden gegeven. Verder is alle communicatie in Signal end-to-end encrypted en zijn zij zeer transparant in de manier waarop zij dit doen.

En de AVG dan?

Signal voldoet niet aan de AVG, aangezien het een Amerikaanse onderneming is en niet onder de Privacy Shield Frameworks valt. Echter, er worden relatief weinig persoonlijke gegevens opgeslagen die ook achterhaald kunnen worden tot een persoon. Signal helpt een bedrijf dus niet direct met het AVG proof worden.

Is dit geschikt voor mijn bedrijf?

Dit is afhankelijk van uw behoeften. Signal biedt tot 10 deelnemers aan een groepsgesprek, maar nog geen mogelijkheid om met meer dan 2 personen te (video)bellen. Daarnaast biedt het geen koppelingen met bijvoorbeeld Microsoft 365 of vergelijkbare programma's of een locatie om bestanden met elkaar te delen.
Wat Signal wel heeft is dat zij zeer transparant zijn in het delen van hun code. In theorie is het mogelijk om deze code te kopiëren en zelf te hosten, zodat maximale controle over de manier van communiceren bereikt kan worden. Voorwaarde hiervoor is wel dat materiaal (een eigen server) en kennis van het inrichten van servers beschikbaar is.

Uit dit korte onderzoek blijkt dat Signal in principe een prima vervanging zou kunnen zijn voor een Whatsapp als privacy hoog in het vaandel staat. Door de extra toegevoegde beveiliging is het in theorie veiliger te noemen dan Whatsapp, maar let wel op de volgende punten:

- Deel zeer gevoelige informatie het liefst niet via een messaging service.
- Maak gebruik van de extra beveiligingsopties zoals de biometrische identificatie mogelijkheden elke keer dat de app afsluit.

Hoe veilig is Skype for Business?

Skype for Business (hierna Skype) is een van de bekendste videovergaderingsapplicaties en wordt bij veel organisaties als standaard gebruikt. Hoe zit het eigenlijk met de veiligheid van Skype?

Wat belooft het?

Skype belooft chatten, online vergaderen en gemakkelijk te installatie. Met de overgang naar Teams, welke Microsoft promoot, is het installeren nog niet heel erg eenvoudig. De consumenten versie is gemakkelijk te vinden, maar de 'for business' versie is lastig te vinden op de Microsoft sites. De ondersteuning voor Skype stopt per 31 juli 2021.

Manier van inloggen?

Skype is net zoals Teams gekoppeld aan het Microsoft 365 account. Dat wil zeggen dat als er al ingelogd is met het Microsoft account er automatisch wordt ingelogd bij Skype (Single Sign-On).
Wanneer niet is ingelogd met een bestaand Microsoft 365 account, worden de inloggegevens en eventuele Multi-Factor Authentication gebruikt van het Microsoft account . Dit biedt de mogelijkheid om over de hele Microsoft omgeving dezelfde vereisten voor de beveiliging in te stellen. Tevens is het mogelijk om een gastaccount te maken voor een vergadering. Voorwaarde is wel dat de organisator over een Microsoft account beschikt.

Wat wordt van mij opgeslagen en hoe?

Skype verzamelt redelijk wat gegevens zoals: NAW gegevens, demografische gegevens, apparaat- en verbruiksgegevens, uw zoekacties en opdrachten, spraakgegevens en locatiegegevens om maar een greep uit het assortiment te doen.

Hierbij komt dat alleen gebruik wordt gemaakt van versleuteling tussen de server en de gebruiker en niet end-to-end. Microsoft heeft dus de mogelijkheid om data in te zien De data wordt volgens Microsoft enkel gebruikt om de diensten te verbeteren.

En de AVG dan?

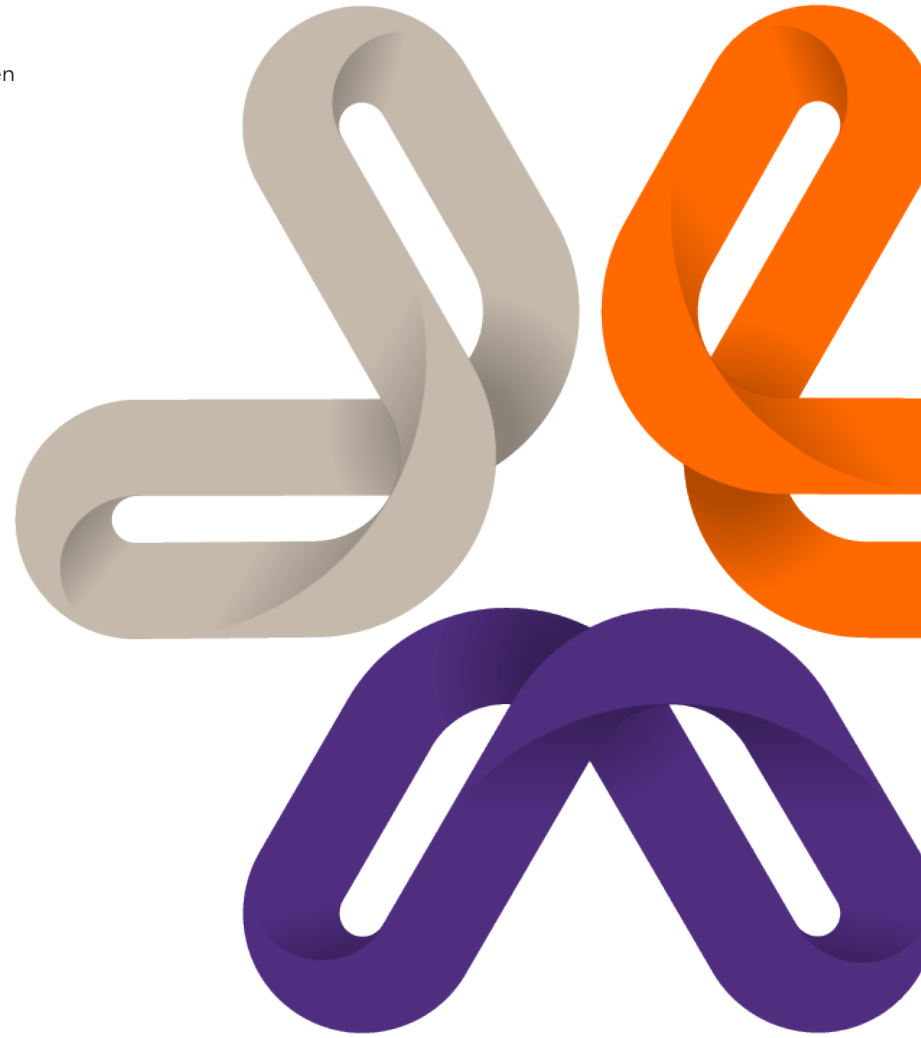
Microsoft is AVG proof, in de zin dat data binnen de EU wordt opgeslagen, zij een privacyverklaring hebben en beperkt gegevens verstrekken aan derde partijen (enkel de overheid als hier vanuit een wettelijk perspectief noodzaak voor is). De locatie van de data is inzichtelijk voor de group controller. Het is ook mogelijk om de data van Skype op een eigen server op te slaan.

Skype wordt per 31 juli 2021 vervangen door Teams en stopgezet door Microsoft. Daarnaast zijn de functionaliteiten als het gaat om digitaal samenwerken aanzienlijk beperkter in Skype dan in Teams. Zo is er wel een functionaliteit om via Outlook een vergadering in te plannen via Skype, maar houdt het hier ook mee op. Bestanden delen met collega's gaat log en chatgesprekken kunnen moeilijk teruggevonden worden. Qua veiligheid is Skype gelijkend aan Teams en is dit zeer afhankelijk van de instellingen in de gehele Microsoft omgeving. Met de volgende tips kan Skype veilig worden genoemd:

- Maak gebruik van een sterk wachtwoord en Multi-Factor Authentication.
- Sla communicaties waarin bedrijfsgevoelige informatie besproken wordt op in een extra beveiligde omgeving.

Wanneer u meer informatie wilt over videoconferencing tools in relatie tot een veilige werkomgeving? Neem dan gerust contact op met ons. We helpen u graag op weg met deze nieuwe manier van samenwerken.

Deze leidraad is opgesteld door Wen Bruins, Junior consultant en Ruben Raijer, Senior consultant. Beiden werkzaam bij Cyber risk services Grant Thornton.



Contact

Migiel de Wit-Beets
Partner
T 088 676 91 86
E migiel.de.wit@nl.gt.com

Grant Thornton