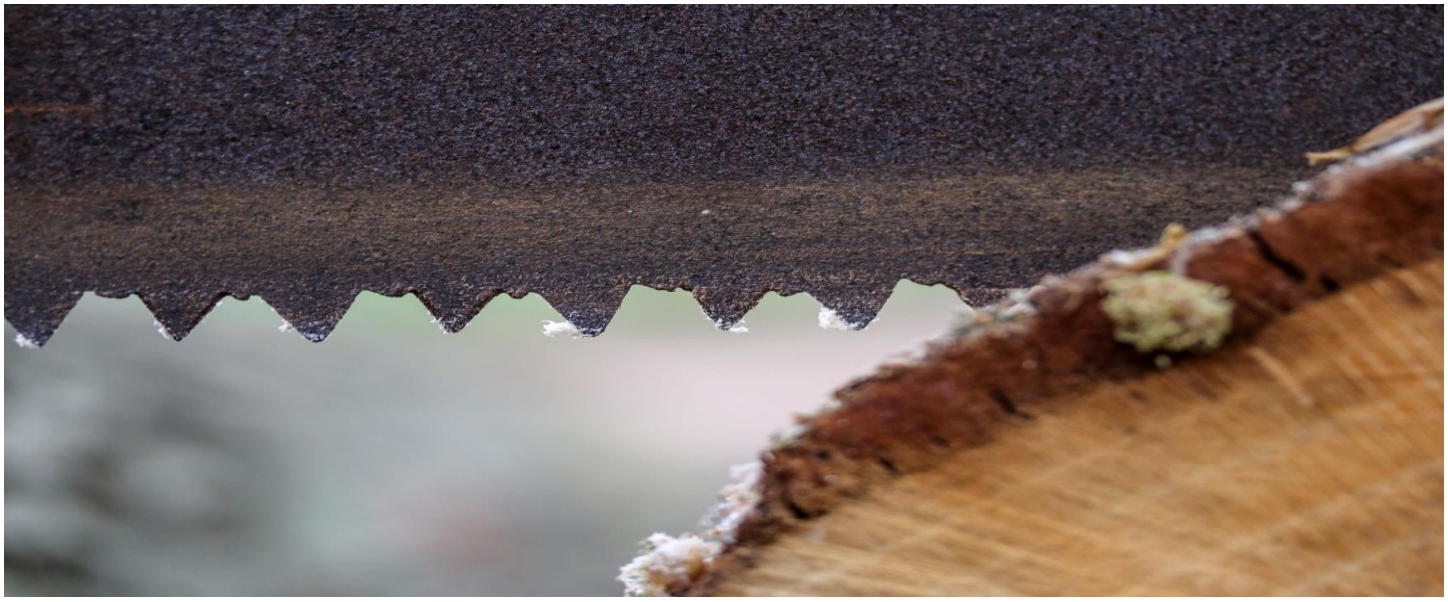

Up-a-Tree en video-vergaderen

Door de corona crisis is onze dagelijkse werkomgeving ingrijpend veranderd. Waar we ‘vroeger’ veel contact hadden in het fysieke domein, is dit snel veranderd. Noodgedwongen voert nu de digitale maat de boventoon.

Up-a-Tree gebruikt ook in coaching sessies, trainingen en vergaderingen vormen van video-vergaderen. Een aantal vragen die daarbij aan ons gesteld worden behandelen we in deze folder.

Het gaat over privacy aspecten en de do’s-and-dont’s bij een video-vergadering. Op deze pagina vindt u hiernaast al een aantal etiquetteregels om een video-vergadering te verbeteren.

Hieronder zetten we uiteen welke aspecten Up-a-Tree heeft beoordeeld en hoe de keus voor een platform gemaakt is.

Up-a-Tree
ASSOCIATES

TIPS VOOR EEN PRETTIGE VERGADERING

GA IN EEN RUSTIGE OMGEVING ZITTEN

*

ZORG VOOR EEN RUSTIGE ACHTERGROND

*

TEST UW CONFIGURATIE VOOR BEELD EN GELUID VÓÓR U DEELNEEMT

*

ZET UW MICROFOON ALLÉÉN AAN ALS U HET WOORD NEEMT

*

www.up-a-tree.nl
contact@up-a-tree.nl

Uitgangspunten voor video-vergaderingen

Video-vergaderen heeft bedreigingen en kansen. Hier zetten we enkele aspecten op een rij m.b.t. A. aspecten van Techniek, Veiligheid en Privacy, B. Gebruiksuitgangspunten en C. Keuze.

A. Aspecten van Techniek, Veiligheid en Privacy

Bij de keuze voor een systeem is een aantal kernvragen van belang:

I. *Is de verbinding beveiligd met encryptie? (bijv. https:// of AES-256 coderingen)* Een encrypted verbinding maakt dat de video/geluidsstream van gebruiker naar gebruiker is versleuteld. Daardoor is deze beschermd tegen ongewenste en ongeoorloofde inbreuken.
II. *Geeft de dienst de mogelijkheid om een datacenter aan te wijzen in de Eurozone, zodat deze onder de Europese AVG/GDPR richtlijnen valt?* Video-vergaderen heeft altijd een server nodig, als spin in het web. Zolang deze binnen de EU wordt gehost, valt deze onder de GDPR richtlijnen, en dus onder de AVG. Dit geeft handvatten over de veilige opslag van gegevens, het beschikkingsrecht en de privacy aspecten ervan.
III. *Hoe is het privacy beleid opgezet en gewaarborgd?* Wat heeft de leverancier van de dienst vastgelegd over hoe zij omgaat met de gegevens waarover ze beschikt van u en uw video conferenties? Voor u belangrijk om te toetsen of dit past bij het doel waarvoor u de dienst wil gebruiken.

B. Gebruiksuitgangspunten

Hoe u omgaat met de videodienst is ook van belang.

I. Zoek bij voorkeur een rustige omgeving (zoals een studeerkamer) op.
II. Zorg dat de achtergrond neutraal is.
III. Stel de videovergadering zo in dat deze maximaal is beveiligd:
    - Gebruik bij voorkeur iedere keer een verse ‘videokamer’. Dus niet doorgaan met de settings van de vorige keer.
    - Stel een uniek toegangswachtwoord in dat u iedere keer opnieuw deelt.
    - ‘Sta bij de deur’: Zorg ervoor dat er een wachtkamer is, zodat u degene bent die mensen binnen laat.
    - Doe de deur dicht: sluit een kamer ‘af’ voor toegang zodra iedereen ‘binnen’ is. Dit voorkomt dat er (per ongeluk) ongewenste personen binnen komen.
    - Als u Wifi gebruikt: gebruik een goed beveiligd netwerk, en zeker geen openbaar access point.
    - Optioneel: Stel de vergadering zo in dat er geen schermen gedeeld kunnen worden. Zo kunt u ook niet per ongeluk privacy gevoelige zaken op uw scherm delen.
    - Optioneel: Maak duidelijk kenbaar dat deze vergadering niet wordt opgenomen. Maak dat bij voorkeur onmogelijk door de optie uit te schakelen voor deze vergadering.

C. Keuze: Welke video-dienst heeft de voorkeur?

Gelet op bovenstaande uitgangspunten hebben we bij Up-a-Tree gekeken naar de betaalde versies van Zoom, MS Teams en Google Hangouts. De gratis aangeboden diensten hebben vaak weinig instelmogelijkheden, bieden geen privacy-voorwaarden en zijn dus ‘ongrijpbaar’ als het gaat om beveiliging- en privacy aspecten. Gelet op techniek, veiligheid, privacy, instelbaarheid en gebruiksgemak komt voor ons Zoom als nummer 1 uit de bus. Microsoft Teams is goede tweede, die we dan ook in andere bijeenkomsten gebruiken. Google Hangouts, het goedkopere alternatief, gebruiken wij niet.

Garantie tot de router…

Bied dit nu een 100% garantie? Het volgen van bovenstaande punten geeft helaas geen garantie dat het altijd goed gaat. De invloed van de gebruiker gaat niet verder dan de persoonlijke router. Voor alles daarbuiten zijn we afhankelijk van een complex geconfigureerd netwerk dat internet heet, waarbij data afgehandeld worden door een keten aan partijen: uw provider, de landelijk netbeheerder, een datacentrum, uw software leverancier, etc. Keuzes waar u niet altijd invloed op heeft. Dit alles bij elkaar bepaalt de veiligheid van ons internet. In de praktijk gaat daar heel veel in goed. Soms helaas niet. Tenslotte: De kans op hackers kan wel verkleind worden door eenvoudige maatregelen:

- Controleer hoe u de instellingen van uw apparaten en software kunt gebruiken voor de beste bescherming.
- Houdt de computer up-to-date met de laatste (systeem) software
- Gebruik niet te eenvoudige wachtwoorden, of overal dezelfde wachtwoorden

Het is mogelijk dat gezien de snelle ontwikkelingen op het gebied van thuiswerken en video-vergaderen ons standpunt aangepast moet worden. Dat zal dan op deze plaats gemeld worden en in de praktijk doorgevoerd worden.

Mei 2020