ZOOM zo veilig mogelijk gebruiken
Problemen en oplossingen

Na wat speurwerk over ZOOM volgt hier het beleid met betrekking tot het gebruik van ZOOM binnen de Inspraak. Op deze manier proberen we ZOOM zo veilig mogelijk te gebruiken. Eerst worden de problemen opgesomd die bekend zijn van ZOOM met daarbij de mogelijke oplossingen. Vervolgens vertaalt dit zich in een beleid wat De Inspraak zal gaan voeren.

PROBLEMEN EN OPLOSSINGEN:

Probleem 1:
- ZOOM aanvallers wonen open meetings bij en delen ongewenste content (ZOOM-bombing)

Te voorkomen door:
- Tips voor HOST: Instellingen binnen je ZOOM account aanpassen:
  - gebruik wachtwoord
  - mute deelnemers op moment dat ze de meeting binnenkomen
  - schakel schermdelen uit zodat deelnemer jouw meeting niet kan overnemen op zijn of haar eigen scherm zonder jouw toestemming
  - (in principe niet nodig als je jouw ZOOM account voldoende beveiligd: je kunt een deelnemer uit je ZOOM meeting verwijderen: klik op 'Bewerk deelnemers' onderaan je ZOOM scherm. Naast de naam van de persoon die je wilt verwijderen klik je op MORE. Je selecteert REMOVE en na bevestiging is de deelnemer uit je room.
  - wees voorzichtig met het delen van ZOOM links; deel ze niet op openbare plaatsen; hackers zoeken daarnaar. Deel ze alleen met degene die je daadwerkelijk toegang wilt geven.
  - Lock je meetings in ZOOM. Als iedereen binnen is; klik dan op Security onderaan en kies voor Lock Meeting. Als jij een meeting afsluit, kunnen geen nieuwe deelnemers meer aansluiten, ook niet als zij een meeting-ID hebben en een wachtwoord hebben.
  - Maak gebruik van de wachtkamer: iedereen die de meeting binnenkomt wordt eerst in de wachtkamer geplaatst en moet worden geaccepteerd door de host.
- Tips voor DEELNEMER:
  - gebruik ZOOM chats niet voor privéberichten: de meeting kan worden opgenomen. De Host ontvangt na de meeting een transcriptie van alle berichten die zijn verstuurd.
  - deel geen persoonlijke te herleiden informatie; alles wat je zegt kan opgenomen worden
  - zet video uit en mute jezelf zolang het kan
  - download geen files via ZOOM
  - gebruik een alias in plaats van je echte naam

Zie voor meer tips: https://www.youtube.com/watch?v=JvTMA6d-LwU&feature=emb_title

Probleem 2:
- ZOOM deelt data met Facebook via hun iOS app

Te voorkomen door:
- Niet inloggen via Facebook account
- ZOOM heeft hier zelf al een oplossing voor; deze datadeling gebeurt niet meer

Probleem 3:

Een aanvaller kan de Windows login-gegevens stelen van andere gebruikers
Te voorkomen door: dit was alleen mogelijk op het moment dat iemand in de groepschat een link stuurde. Als iemand dan op deze link klikte kon Windows een poging doen om te connecten en via dat proces was het voor een aanvaller eventueel mogelijk om je wachtwoord te achterhalen. Zoom heeft dit aangepast, dit kan nu niet meer. Door geen links te delen in je chat voorkom je dit ook zelf.

Probleem 4:
Het is eenvoudig om LinkedIn-profielen van deelnemers van vergaderingen te achterhalen
Te voorkomen door: voorkomen is niet meer nodig; deze optie is inmiddels gedicht.

Probleem 5:
Hosts kunnen hun ZOOM-meetingen opnemen zonder dat alle deelnemers dat weten of daar toestemming voor geven. Opgeslagen videos kunnen buiten het ZOOM netwerk eenvoudig worden teruggevonden; de inhoud van de meeting ligt dan op straat.
Te voorkomen door: afspraak maken dat er niet iets zonder toestemming wordt opgenomen. Alle functies van Recording uitschakelen.

Probleem 6:
Men kan onbevoegd bij login-gegevens komen, toegang tot microfoon en camera van deelnemers krijgen en onbevoegd berichten lezen.
Te voorkomen door:

- Aanpassen van profielinstellingen:
  - houd je 'Meeting ID' privé en deel het via een andere bron met mensen die je in de meeting wil hebben
  - beveilig je 'meeting id' met een wachtwoord
  - zet optie 'Scherm delen' op 'Host Only' (dit voorkomt ZOOM bombing)
  - zet mensen digitaal in de wachtkamer, de host bepaalt wie er mee gaat doen
  - door een virtuele achtergrond te kiezen voorkom je dat deelnemers in jouw kamer kunnen kijken

Probleem 7:
In ZOOM zijn een aantal features die het voor de host mogelijk maken om aanvullende gegevens te verzamelen.
Hoe gaan we hiermee om:
De Inspraak zal de afspraken waar zij zich aan zullen committeren transparant communiceren naar de cliënt (zie beleid - Afspraken).

Probleem 8:
Er lekken e mailadressen van gebruikers naar andere gebruikers => probleem opgelost.
Update 10 april 2020: andere mailadressen zijn niet langer zichtbaar binnen de nieuwste versie van ZOOM. Zie onderstaande blog voor meer informatie
https://blog.zoom.us/wordpress/2020/04/08/zoom-product-updates-new-security-toolbar-icon-for-hosts-meeting-id-hidden/

Probleem 9:
Zoom legt geen verantwoording af over inzageverzoeken van overheden.
Te voorkomen door: dit is niet te voorkomen, maar ook niet gelijk een groot probleem. Zoom heeft de technische mogelijkheid om eventueel, als de overheid dat vraagt, video- of chatmateriaal aan de overheid te geven als dit wettelijk wordt gevraagd. Sommige grote bedrijven maken een verslag met welke overheidsorganen dit aan ze vragen. Zoom heeft dit nog niet gedaan, maar dat betekent niet dat dit niet alsnog gaat komen nu het aantal gebruikers zo is gestegen.

Aanvullende tips:

- gebruik alleen de laatste versie van ZOOM vanwege updates op gebied van veiligheid.
- gebruik alleen meeting specific meeting-IDs, no general Meeting-IDs

Zoom is Privacy Shield- en SOC2 tpe II-gecertificeerd. Dit geldt als een goede privacy standaard voor een Amerikaanse dienstverlener.