

Brug af kommunikations- og samarbejdsplatforme

Skype for Business, Slack, Microsoft Teams, WhatsApp, Starleaf og andre lignende platforme til kommunikation og samarbejde anvendes i stor stil som følge af den nuværende corona-situation, hvor det frarådes at mødes fysisk.

Det samme gør sig gældende for fildelingstjenester, som enten er integreret i samarbejdsplatformene eller stand-alone som Dropbox, iCloud m.fl.

Ingen af disse platforme er generelt sikkerhedsteknisk undersøgt, valideret eller godkendt af Center for Cybersikkerhed. Det er heller ikke en forudsætning for deres brug, at de er godkendte, medmindre de skal anvendes til klassificeret information jf. Justitsministeriets sikkerheds-cirkulære.

Ikke desto mindre bør myndigheder og virksomheder være opmærksomme på en række forhold omkring samarbejdsplatformene.

Center for Cybersikkerhed anbefaler, at der foretages en risikovurdering af anvendelsen af kommunikations- og samarbejdsplatforme, inden de tages i brug. Dette gælder især, hvis de skal anvendes til at behandle oplysninger af beskyttelsesværdig eller sensitiv karakter.

Brugerinformationer og data, der anvendes herunder opbevares, på platformene, er underlagt platformens brugerbetingelser (EULA), der kan indebære datamining og andre platformsafhængige betingelser. Disse forhold bør derfor indgå som et centralt element i risikovurderingen.

Kommunikationen på disse platforme er typisk krypteret. Center for Cybersikkerhed anbefaler dog, at platformene betragtes som værende usikre. Overvej derfor nøje, hvilke oplysninger der kan behandles via disse tjenester.

Selvom sikkerhedsevaluering ikke er en forudsætning for anvendelse af platformene, kan anden lovgivning f.eks. persondatareguleringen stille krav til, hvilke og hvorledes platformene kan anvendes.

Det anbefales derfor, at virksomheder og myndigheder melder klart ud til deres medarbejdere, hvilke platforme der efter risikovurderingen kan anvendes til arbejdsrelateret samarbejde. I forlængelse heraf bør der fastsættes interne regler for, hvilke informationer, der kan deles på platformene og hvordan. Husk at kommunikere reglerne ud til hele organisationen.

Dato: 24. marts 2020

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cfcs@cfcs.dk
www.cfcs.dk

Endelig anbefaler Center for Cybersikkerhed ved fraværet af selvstændige sikkerhedsevalueringer, at der anvendes internationalt anerkendte samarbejdsplatforme fra større leverandører.

Find mere information om at arbejde på distancen

- Råd om sikkerhed på mobile enheder: <https://fe-ddis.dk/cfcs/publikationer/Documents/Mobilsikkerhed.pdf>
- Gode råd om hjemmearbejde: <https://fe-ddis.dk/cfcs/publikationer/Vejledninger/Pages/Gode-raad-om-hjemmearbejde.aspx>
- Cybersikkerhed ved hjemmearbejde: <https://fe-ddis.dk/cfcs/publikationer/Vejledninger/Pages/Cybersikkerhed-ved-hjemmearbejde.aspx>