Guide inför digitala möten utifrån ett informationssäkerhetsperspektiv

Den här guiden syftar till att medarbetare och politiker ska kunna hantera verksamhetens information korrekt i digitala möten. Guiden är framtagen i samverkan med V6-kommunernas informationssäkerhetssamordnare och säkerhetssamordnare från Räddningstjänsten Västra Skaraborg samt Göliska IT. Guiden kommer att kompletteras och uppdateras varför utskrifter riskerar att bli gamla och ofullständiga. För mer info kontakta informationssäkerhetssamordnare på 073-344 61 93 eller via mejl ulrika.helgesson@goliskait.se

Det finns flertalet verktyg för distansmöten som klarar av videosamtal, chatt med mera. Inom V6 används företrädesvis Skype for business som är säkert och supporterat av Göliska IT. Ett annat vanligt förekommande verktyg är Microsoft Teams där möten skapas och bjuds in till från organisationer/användare som använder O365.

Ytterligare verktyg som används är Zoom. Zoom används vanligtvis inom utbildningssektorn. Därutöver finns fler verktyg vilka inte omfattas av denna guide.

Generellt gäller:

- Vid möten med information som rör Sveriges säkerhet ska Skype ALDRIG användas. Kommunens/Göliska IT:s säkerhetssamordnare ger ut instruktion om vad som gäller.

- Följ SKR:s råd vid digitala möten, se nedan.

- Om det finns lagar som ställer särskilda krav förväntas respektive verksamhet känna till och följa dessa. Exempelvis anger författningssamlingen HSLF-FS att verksamhet som lyder under denna har krav på stark autentisering (tvåfaktorsinloggning eller motsvarande) vilket Skype i sig inte har.

I övrigt ska man tänka på att agera som i ett vanligt fysiskt möte, det vill säga:
- spela inte in mötet,
- säkerställ att endast behöriga mötesdeltagare finns med i mötet och att dessa får ta del av den information som är tänkt att avhandlas,
- säkerställ att ingen obehörig kan höra eller se information i mötet utan att vara med via Skype,
- observera att om du delar din kalender med hög behörighet till andra är även möten med länkar till exempelvis Skype och Teams tillgängliga för dem.

Se även SKR:s råd vid digitala möten:
- Gör alltid en bedömning om mötet ska genomföras fysiskt eller digitalt. Bedömningen ska göras utifrån mötes innehåll, deltagare och individens behov. Skyddsbedömningar gällande barn ska till exempel inte ske digitalt.
- Tänk över hur den enskilde ska identifiera sig (till exempel genom att visa upp sin legitimation i bild vid nybesök).
- Ta hänsyn till integritet, sekretess och säkerhetsfrågor.
- Se till att medarbetare som arbetar hemifrån ansluter sig till kommunens VPN, och att de säkerställer att miljön de sitter i tar hänsyn till integritet och sekretess.

- Dela aldrig dokument med känsliga personuppgifter via appar eller i chattfunktioner, varken med den enskilde eller andra aktörer.

Skype for business

Villkor för säker Skype-användning

1. Alla mötesdeltagare måste använda **Skype for business** från Göliska IT. Det är en version som kräver licens och som finns installerad på alla kommunens datorer, förtroendevaldas surfplattor och i vissa fall även på smartphones.
2. Alla mötesdeltagare måste **logga in med sitt kommunala användarkonto/AD-konto**.
3. Användare som blir inbjudna till ett Skype-möte där mötesbokaren är utanför Göliska IT:s miljö kommer att åtnjuta den bokande organisationens säkerhetsinställningar.

Om villkoren för punkt 1 och 2 ovan är uppfyllda spelar det ingen roll varifrån man deltar i mötet. Mötet är säkert även när man befinner sig utanför arbetsplatsen och de kommunala nätverken. En rekommendation är ändå att använda den utrustning som kommunen tillhandahåller.

Denna guide har enbart utgått från att krav kring att teknik och konfidentialitet är analyserade. Analysen klargör att information som hanteras i ljud och bild via Skype tekniskt sett inte kan avlyssnas av obehöriga. Anledningen till att tillgänglighet och riktighet inte varit relevanta att analysera har att göra med att ingen information lagras, bearbetas etc.
Generellt gäller att:

- Skype har en hög teknisk säkerhetsnivå förutsatt att villkoren ovan är uppfyllda och lever då upp till kravnivå 3 som är den högsta skyddsnivån enligt SKR:s KLASSA-metod.
- Om ovanstående villkor för säker Skype-användning är uppfyllda kan Skype användas för alla möten och för hantering av all information.

Microsoft Teams-möten

Framtagningen av guiden har enbart utgått från att de tekniska kraven samt konfidentialitetsaspekten av informationssäkerhet är analyserat. Det betyder att information endast ska ha möjlighet att nås av behöriga användare. Nedan förkortas Microsoft Teams till endast “Teams”.

OBS, denna guide gäller digitala möten och den information som förmedlas där. Det vill säga att dokumenthantering i Teams inte omfattas.

Analysen klargör att information som hanteras i ljud och bild via Teams tekniskt sett inte kan avlyssnas av obehöriga om leverantören lever upp till sina driftsåtaganden, se Krav från riskanalys nedan. Generellt gäller att:

- Teams har en hög teknisk säkerhetsnivå förutsatt att vissa villkor är uppfyllda och lever då upp till kravnivå 3 som är den högsta skyddsnivån enligt SKR:s

KLASSA-metod. Se Villkor för Teams-användning längre ner på sidan.

- Om villkoren för säker Teams-användning är uppfyllda kan Teams användas för alla möten och för hantering av all information.

Villkor för säker Teams-användning

- Den som bokar möten och bjuder in andra mötesdeltagare måste använda **Teams** från Göliska IT. Det är en version som kräver licens. Gäller för användare med O365-licens.
- Alla mötesdeltagare måste **logga in med sitt kommunala användarkonto/AD-konto**.
- Användare utan O365-licens kan bli inbjudna till ett Teams-möte. För dessa möten uppnås samma säkerhetsnivå som för en licensierad användare.
- Om ovanstående villkor är uppfyllda spelar det ingen roll varifrån man deltar i mötet. Mötet är säkert även när man befinner sig utanför arbetsplatsen och de kommunala nätverken. En rekommendation är ändå att använda den utrustning som kommunen tillhandahåller.
- Krav från riskanalys: För nedanstående krav på säkerhetsåtgärder har vi/Göliska IT inte verifiering från Microsoft utan vi förlitar oss på deras hantering/kapacitet för dessa krav.
- Utvecklings- och testsystem skyddas antingen på likvärdigt sätt som produktionssystemet, alternativt innehåller inte konfidentiell eller känslig information.
- Systemets resursanvändning och prestanda övervakas.
- Alla större ändringar utvärderas i en testmiljö innan de installeras i produktionsmiljön.
- Nätverkssegmentet där systemet är placerat motsvarar skyddsnivån för betydande påverkan.
- Riktlinjer för säker systemutveckling för systemet finns dokumenterade och efterlevs.
- Systemet har tillräcklig redundans för att uppfylla tillgänglighetskrav.

Zoom

Zoom är ytterligare en tjänst för distansmöten och finns att använda dels som gratisversion dels som en licenserad produkt för organisationer.

Framtagningen av guiden har enbart utgått från att de tekniska kraven samt konfidentialitetsaspekten av informationssäkerhet är analyserat. Det betyder att information endast ska ha möjlighet att nås av behöriga användare.

Analysen klargör att information som hanteras i ljud och bild via Zoom tekniskt sett inte kan garanteras och att det kan avlyssnas av obehöriga.

Generellt gäller att:

- Zoom har en teknisk säkerhetsnivå som bedömt lever upp till kravnivå 0 vilket är den lägsta skyddsnivån enligt SKR:s KLASSA-metod.

I övrigt ska man tänka på att agera som i ett vanligt fysiskt möte, det vill säga:

- den enskilde medarbetaren ska tillsammans med sin chef/informationsägare göra en bedömning i varje fall angående vilken information som kan kommuniceras eller om deltagande överhuvudtaget är aktuellt.
- Om du blir inbjuden till ett möte med en och får en länk är det viktigt att du säkerställer att länken verkligen går till Zoom och inte till en bedragare som försöker få dig att installera skadlig kod på datorn.
- Om du har fått en länk med en webbadress ska du alltid kontrollera att länken börjar med http://us04web.zoom.us.
- Om du inte fått en länk med en webbadress får du i stället säkerställa att inbjudan är korrekt. Förväntar du dig en mötesinbjudan från personen? Känner du till personen som skickat inbjudan? Vid minsta tvekan – ta kontakt med personen eller organisationen för att säkerställa att det är korrekt.

Deltagande i andra digitala möten

Det finns ett flertal andra lösningar för digitala möten. För dessa kan vi inte uttala oss om säkerheten vilket innebär att särskild försiktighet måste iakttas. Då medarbetare får mötesinbjudningar från externa parter via andra verktyg än Skype och Teams måste den enskilde medarbetaren tillsammans med sin chef/informationsägare göra en bedömning i varje fall angående vilken information som kan kommuniceras eller om deltagande överhuvudtaget är aktuellt.