CENTER FOR CYBERSIKKERHED

DIGITALISERINGSSTYRELSEN

God kultur ved distancearbejde

Som medarbejder spiller du en vigtig rolle for den samlede sikkerhed i den organisation, hvor du arbejder.

Traditionelt har organisationens regler, retningslinjer og rutiner for informationssikkerhed taget udgangspunkt i en arbejdssituation, hvor det primære arbejdssted er på kontoret i fysisk nærhed af kolleger og it/sikkerhedsansvarlige kolleger.

I takt med at arbejdet flytter hjem eller ud i byen, er disse regler, retningslinjer og rutiner ikke nødvendigvis dækkende eller tilstrækkelige for at opretholde organisationens sikkerhed. Derfor er der behov for, at du som medarbejder er opmærksom på dine rutiner og din adfærd, så du – uanset hvor din fysiske arbejdsplads er – kan bidrage til at opretholde et højt sikkerhedsniveau i din organisation.

Center for Cybersikkerhed og Digitaliseringsstyrelsen giver dig herunder en række konkrete bud på, hvad du som medarbejder selv kan gøre for at øge sikkerheden, når du gør brug af distancearbejde. Hvis du er i tvivl om, hvordan du efterlever rådene, bør du spørge din it-support eller it-sikkerhedsfunktion, hvis der er en sådan. Hvis det ikke er tilfældet, må du hente hjælp hos din chef eller anden med ledelsesansvar.

1. Politikker for distancearbejde

1.1 Læs og følg din organisations sikkerhedspolitikker for distancearbejde

Din organisations sikkerhedspolitikker afspejler ledelsens syn på, hvordan du på sikker vis kan og må arbejde fra eksterne lokaliteter herunder hjemmefra. Når du arbejder fra eksterne lokaliteter, vil det kunne udfordre organisationens sikkerhed. Du bør derfor sætte dig ind i din organisations sikkerhedspolitikker på området. Hvis din organisation ikke har en politik eller nogle retningslinjer på området, kan du opfordre til, at I får nogle. Det er ledelsens ansvar at sikre, at du kan arbejde sikkerhedsmæssigt forsvarligt.

2. Brug for hjælp i forbindelse med distancearbejde?

2.1 Er der udfordringer med din distancearbejdsplads? Så brug de muligheder for hjælp, som din organisation stiller til rådighed.

Som medarbejder kan man let stå i en situation, hvor den tekniske platform til distancearbejde ikke fungerer efter hensigten. Nogen vil måske prøve at løse problemet eller omgå det ved egen eller en kollegas hjælp. Måske bliver problemet løst – men reelt set betyder det, at organisationens it- og supportfunktion ikke får viden om potentielle problemer eller udfordringer, som mange medarbejdere måske kæmper med. Derfor bør du som medarbejder bidrage til videnopsamling ved at søge hjælp i support-funktionen. Hermed kan du være med til at sikre, at din distancearbejdsplads på sigt bliver forbedret og mere sikker.

3. Arbejdsmøder i det offentlige rum

3.1 Brug privacy-filter på din computer/tablet/mobil.

Shoulder surfing - det at kigge nogen bevidst eller ubevidst over skulderen - er en udbredt udfordring, når man arbejder i det offentlige rum. Et privacy-filter er et specielt stykke gennemsigtigt folie som sættes uden på skærmen og er med til at reducere uønsket indblik på dine mobile enheder.

3.2 Hav høretelefoner på, når du deltager i et digitalt møde i det offentlige rum.

Ved at bruge høretelefoner sikrer du, at eventuelle uvedkommende tilhørere kun får adgang til den ene del af samtalen. Det er med til at beskytte dine samtalepartnere og deres informationer. Samtalekvaliteten bliver typisk også bedre.

3.3 Tal ikke om sensitive emner i det offentlige rum.

Når du arbejder fra caféer, hoteller, tog og busser kan alle lytte med. Det øger risikoen for, at uvedkommende får adgang til fortrolige oplysninger om produkter, data, kolleger og samarbejdspartnere. Dette gælder både digitale og fysiske møder. Det samme kan være tilfældet ved hjemmearbejde.

3.4 Brug VPN

Når du tilgår organisationens interne netværk udefra bør du i samarbejde med din organisation sikre dig, at kommunikationen til og fra din organisations interne systemer er sikret med VPN. Når du anvender VPN er kommunikationen mellem din mobile enhed og din arbejdsplads krypteret, således at uvedkommende ikke kan få indsigt i, hvad der overføres. Er du i tvivl om, hvorvidt du kan/skal anvende VPN, og hvordan du gør det, så spørg din it-support-funktion. Det vil ofte også fremgå af organisationens it-sikkerhedspolitik.

3.5 Brug åbne offentlige WIFI-netværk med omtanke

Åbne offentlige netværk anses som udgangspunkt for usikre, da man som bruger ikke kan være sikker på, hvem der reelt står bag et givent netværk, og hvordan sikkerheden i øvrigt er håndteret. Brug i stedet (hvis muligt) internetdeling via din mobiltelefon. Husk at beskytte adgangen med en kode.

4. Digitale møder

4.1 Verificér mødedeltagere i digitale møder ved billede eller på anden måde.

Ved online-møder er det let for eksterne deltagere at skjule deres rette identitet bag en avatar eller et falsk ikonbillede. Hvis du er mødeleder i et møde, hvor en mindre gruppe er inviteret, bør du sørge for at identificere eksterne personer, der deltager i mødet. Du kan fx bede dem præsentere sig selv med kamerabillede. Hvis mødelederen ikke sørger for en præsentation, kan du være den, der beder om, at det sker. Ved stormøder, hvor en præsentationsrunde ikke giver mening, kan du styre eksterne deltagere Det kan være nødvendigt – og ofte ligefrem en god ide – at udelukke uidentificerede og ikke-navngivne deltagere, medmindre det strider mod mødets formål.

4.2 Vær opmærksom på, hvad der vises fra din skærm.

Når du deltager i et virtuelt møde og skal præsentere noget for andre mødedeltagere så vær opmærksom på, at du ikke afslører mere end det, du har til hensigt at præsentere. Deling af skærm, program eller præsentation kan i nogen tilfælde give de andre deltagere mulighed for indsigt i noter og andre interne oplysninger. Når du deler din skærm så luk de programmer, der ikke bruges til præsentationen og undgå at vise skrivebordet, så kun præsentationen, billedet eller dokumentet vises for alle deltagere. På den måde kan du styre, hvad du giver andre mødedeltagere indblik i.

5. Undgå læk ved deling af billed- og videomateriale på sociale medier

5.1 Vær opmærksom på risikoen for læk af interne oplysninger

Det er let at komme til at lække interne og sensitive informationer, hvis man poster fx billed- eller videomateriale fra sin arbejdssituation på sociale medier. Vær derfor særligt opmærksom på hvilke arbejdsrelaterede opgaver og oplysninger du deler på sociale medier. Undgå særligt billeder af skærme, kommunikationsudstyr, noter og dokumenter.

6. Sikring af mobiltelefon

6.1 Beskyt din mobiltelefon og informationerne på den.

Mobiltelefonen er en uundværlig del af distancearbejdspladsen. Mange interne informationer sendes til og fra denne enhed. Derfor er det vigtigt at beskytte den mod uautoriseret adgang. Dette bør ske med en sikker adgangskode, fingeraftryk eller ansigtsgenkendelse samt kryptering og en begrænsning i notifikationer fra de apps (herunder mail), der kan indeholde interne informationer.

7. Brugen af beskedtjenester (SMS)

7.1 Undgå at sende følsomme oplysninger på SMS eller lignende beskedtjenester.

Mange er ikke klar over, at de informationer, der sendes via beskedtjenester, i særdeleshed almindelige SMS, fremsendes i klar tekst. Det betyder, at de ikke er beskyttet og kan læses af andre, hvis de opsnappes. Overvej derfor om din besked skal beskyttes og brug i givet fald en krypteret beskedtjeneste.

8. Anskaffelse af udstyr

8.1 Anskaf ikke arbejdsrelateret it-udstyr uden aftale med din egen organisation

Som medarbejder får du ofte stillet en it-løsning til rådighed på din distancearbejdsplads. Valget af denne tekniske platform er med stor sandsynlighed sket ud fra et eller flere funktionelle, økonomiske og/eller sikkerhedsmæssige aspekter. Samtidig kan organisationen opretholde et overblik over udstyr, der indgår i driftsmiljøet, hvilket især er vigtigt ved imødegåelser af angreb. Hvis du mangler udstyr, herunder en anden pc, en ekstra skærm, mere RAM, diske mv. bør du derfor som udgangspunkt gøre brug af din organisations egen indkøbsfunktion. I modsat fald risikerer du, at dit udstyr ikke lever op til din organisations sikkerhedsstandard, og at din organisations eventuelle supportenhed ikke kan hjælpe, hvis der opstår problemer med udstyret.

9. Brug af applikationer.

9.1 Brug kun de applikationer, som din organisation stiller til rådighed.

Som medarbejder får du ofte stillet en række applikationer – herunder virtuelle kommunikations- og samarbejdsplatforme - til rådighed på din distancearbejdsplads. Valget af disse applikationer er, lige som med de fysiske komponenter, med stor sandsynlighed sket ud fra funktionelle og/eller sikkerhedsmæssige overvejelser. Selv om du måske er i stand til at downloade og installere andre applikationer, er dette ikke nødvendigvis et udtryk for, at din organisation opfatter disse applikationer som gode ud fra et sikkerhedsmæssigt perspektiv.

Brug derfor de anviste platforme og følg eventuelle retningslinjer fra din organisation om, hvorledes disse kan og skal anvendes. Mangler du en applikation, så ret henvendelse til din organisation for korrekt anskaffelse.

10. Håndtering af arbejdsrelateret information.

10.1 Arbejdsrelaterede dokumenter bør behandles på samme måde derhjemme som på kontoret.

Benytter du printede dokumenter, USB-nøgler eller andet, og opbevarer du dokumenter og medier derhjemme? Så bør du tænke over, om informationerne er så følsomme eller sensitive, at andre ikke må få indsigt i dem. Hvis det er tilfældet, bør du sørge for at opbevare dem i henhold til sikkerhedspolitikken/retningslinjerne på dit arbejde og bringe dem tilbage til kontoret med henblik på destruktion, når du ikke længere har brug for dem.

11. Rapportering af sikkerhedshændelser

11.1 Vær opmærksom på eventuelle brud på it-sikkerheden og meld mistænkelige hændelser til din organisation.

Mange forsøger at udnytte, at organisationers medarbejdere benytter sig af distancearbejde, og dermed måske er mindre beskyttet af de normale sikkerhedstiltag, som organisationen har etableret. Det er derfor vigtigt at rapportere enhver mistanke om en it-sikkerhedshændelse. Dette bør ske hurtigt, så der kan reageres på situationen, hvis den udvikler sig. Alle kommer til at åbne falske problematiske mails, så der er intet pinligt i at melde det ind. Det er derimod vigtigt, at din organisations sikkerhedsfunktion får viden om, hvor der er sårbarheder, så der kan gøres noget ved det.

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

DIGITALISERINGSSTYRELSEN

Postboks 2193
1017 København K
Telefon: 3392 5200
E-mail: digst@digst.dk