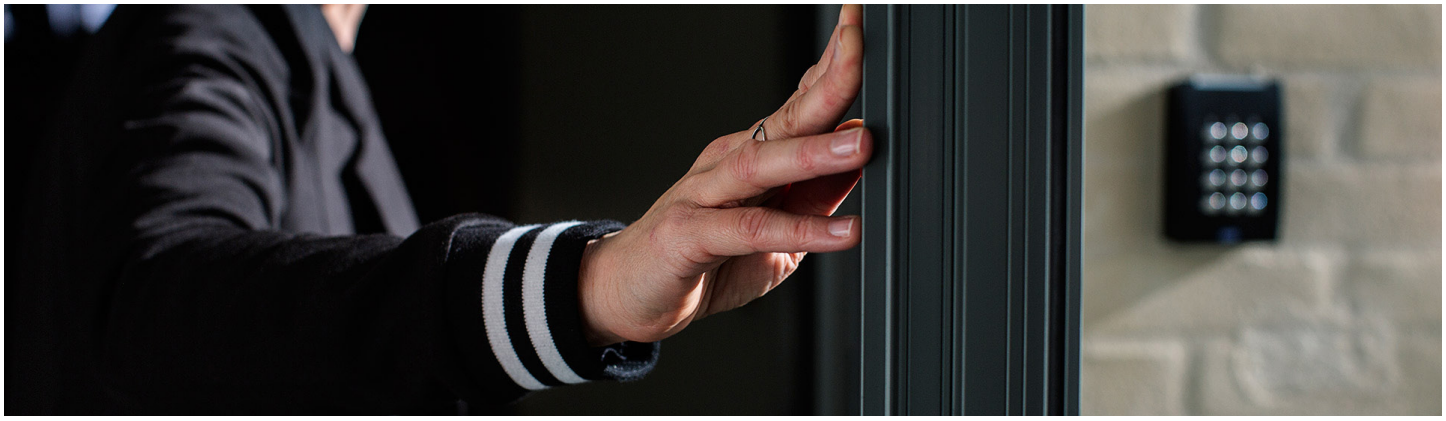

Beskyt jeres organisation, når I modtager besøg

Gode råd til sikkerhed før, under og efter besøg fra udlandet

Samarbejde med udenlandske partnere er en naturlig del af arbejdet i mange organisationer. Videndeling og netværksdannelse i forbindelse med delegationsbesøg kan være af stor værdi, men udgør samtidig en risiko for, at gæsterne uønsket tager beskyttelsesværdige informationer med hjem eller installerer skadelig software på jeres systemer.

Et godt skridt til at beskytte jeres organisation mod uhensigtsmæssig videnoverførsel er at etablere faste procedurer for, hvordan I håndterer besøg. I kan overveje følgende:

Før besøget

1. Overvej risici

Overvej mulige risici ved besøget, og forbered modforanstaltninger.

2. Afgræns adgang til information og områder

Afklar, hvilke informationer der må deles, og særligt, hvilke der ikke må. Afklar, hvilket område besøget skal afgrænses til at foregå i, og efterlad ikke sensitive oplysninger frit tilgængeligt i besøgsområdet.

3. Udpeg opsynsfolk

Udpeg medarbejdere, hvis primære opgave er at holde opsyn under besøget.

4. Tjek, hvem der tager med

Vær opmærksom på deltagerændringer, som meldes ud kort før besøget – især pludselig deltagelse af ambassadepersonale, da efterretningsofficerer kan arbejde under dække af at være diplomater. Også tilrejsende ansatte i myndigheder og andre, som skiller sig ud fra den oprindelige deltagergruppe, bør være et opmærksomhedspunkt.

5. Etabler it-logning
Etabler it-logning for at afklare, om der har været uautoriseret adgang i forbindelse med besøget.

6. Overvej om elektronik må medbringes
Overvej om mobiltelefoner, tablets, kameraer, smartwatches, elektroniske nøgleringe m.m. må medbringes. Disse kan optage lyd og billeder samt registrere gps-positioner, uden I ved det, eller anvendes til at installere skadelig software på jeres systemer.

7. Foretag et baggrundstjek
Foretag et baggrundstjek af nye samarbejdspartnere for at afklare, om der er anledning til bekymring. Det kan fx dreje sig om virksomhedens ejerkreds, anmærkninger i forhold til sanktioner m.v.

Under besøget

1. Sæt tydelige grænser
Begynd med at fortælle jeres gæster om de rammer, som I har sat for besøget, så det er klart for gæsterne, hvad de må og ikke må.

2. Brug gæstebånd
Udstyr gæsterne med gæstebånd eller anden markering, så det er tydeligt, hvem der er besøgende.

3. Hold opsyn med gæsterne
Efterlad ikke gæsterne alene med din organisations elektroniske udstyr – eksempelvis PC, printer, router og servere. Hav opmærksomhed på delegationsdeltagere, der forlader den samlede gruppe eller "farer vild".

4. Tillad ikke installation af fremmed software og hardware
Tillad ikke, at fremmed software og hardware bliver installeret – heller ikke usb-stik i forbindelse med præsentationer. Anvend evt. stand-alone-computere til præsentationer.

5. Vær opmærksom på overraskende spørgsmål
Hav opmærksomhed på spørgsmål, som falder uden for besøgets dagsorden. Det kan fx være spørgsmål om sikkerhed, følsomme politiske emner eller navne på personer.

Efter besøget

1. Gennemgå it-logning
Gennemgå it-logning med henblik på at afsløre uautoriseret adgang til organisationens systemer.

2. Vær opmærksom på efterfølgende kontakt
Vær opmærksom på, om en medarbejder efterfølgende bliver kontaktet af en delegationsdeltager. Giver indholdet af henvendelsen anledning til bekymring? Vær også opmærksom på ønsker fra partneren om gentagne besøg.

3. Evaluer besøget
Evaluer besøget, og reager, hvis I har mistanke om, at der kunne være sket et sikkerhedsbrud eller anden mistænkelig hændelse. Udviste en delegationsdeltager fx en mistænkelig adfærd under besøget? Tag mistanken op med den sikkerhedsansvarlige eller nærmeste leder. Hvis I vurderer, at hændelsen kan relatere sig til spionage eller terrorisme, bør I også anmode PET om et fortroligt møde på *pet@politi.dk* ■

Mere information
Læs mere om spionage i 'Vurdering af spionagetruslen mod Danmark' på *www.pet.dk*

Interesseret i yderligere information om sikkerhed i forbindelse med delegationsbesøg? Bestil en briefing fra PET´s rådgivere via *raadgivning@pet.dk*