ER JERES FORSKNING I FARE?

– Gode råd til forskere og medarbejdere om håndtering af udenlandsk indblanding og spionage

PET

Indhold

Vi skal være bedre rustet

Danmark har et højt niveau inden for teknologi, innovation og forskning, og danske forskningsinstitutioner indgår aktivt i internationalt samarbejde på disse områder. Det er med til at udvikle og bidrage til Danmarks fremtrædende position bl.a. inden for en række forskningsområder. Imidlertid er dansk forskning i skarp international konkurrence, og forskningen kan havne i de forkerte hænder.

Hovedparten af det internationale forskningssamarbejde er til Danmarks fordel. Men der er desværre også eksempler på, at fremmede stater uretmæssigt anskaffer sig viden, teknologi og produkter, som Danmark skal leve af på sigt, eller som kan have en negativ indflydelse sikkerhedspolitisk. Derfor har PET, i samarbejde med Uddannelses- og Forskningsministeriet, udarbejdet en række anbefalinger til jer, der arbejder på forskningsinstitutioner, for at forebygge og håndtere udenlandsk indblanding og spionage.

UDENLANDSK INDBLANDING, SPIONAGE OG PÅVIRKNING

Udenlandsk indblanding *er hemmelige eller problematiske aktiviteter, der udføres af, eller på vegne af, en fremmed stat. Indblandingen er i uoverensstemmelse med Danmarks suverænitet, værdier eller interesser. Det er et bredt begreb, som også omfatter spionage og påvirkning.*

Spionage *er defineret i straffelovens kapitel 12, §§ 107-109. Spionage forstås bl.a. som den aktivitet, hvorved der indhentes eller videregives information om forhold, som af hensyn til den danske stat eller det danske samfunds interesser skal holdes hemmelige. Det forstås ligeledes som spionage, hvis man røber eller videregiver oplysninger, der kan være til fare for fx den danske stats sikkerhed eller samfundsinteresser, eller en herværende enkeltpersons sikkerhed.*

Spionage foregår også, hvis man i øvrigt foretager sig noget, der kan sætte en fremmed efterretningstjeneste – statsligt eller ikke statsligt organiseret – i stand til at virke inden for den danske stats område.

Påvirkningsvirksomhed *sker, når en fremmed stats efterretningstjeneste sættes i stand til at påvirke beslutningstagere eller den almene meningsdannelse inden for den danske stats område. Formålet med påvirkningsvirksomheden kan være at påvirke den offentlige debat eller omverdenens syn på Danmark for at fremme egne interesser på bekostning af danske interesser.*

Truslen er reel

Truslen mod dansk forskning er reel. Gennem de senere år har der været flere eksempler på spionage og anden udenlandsk indblanding. Dansk forskning har en tradition for stor åbenhed og et bredt internationalt samarbejde og kan derfor anses for at være et relativt nemt mål for fremmede stater. Samtidig er Danmark et attraktivt mål på grund af sit høje forskningsmæssige niveau og sin geopolitiske placering.

Visse udenlandske efterretningstjenester har tradition for at infiltrere andre landes forskningsmiljøer, og forskere i de pågældende lande kan være under stærkt pres. Enkelte autoritære stater har desuden love, der pålægger deres lands statsborgere at bistå efterretningstjenesterne med oplysninger af interesse for staten.

PROFESSOREN, DER BLEV DØMT FOR SPIONAGE

I 2010 blev en finsk, samfundsvidenskabelig professor anholdt i et S-tog. Han var ansat på Københavns Universitet og var på vej til et møde med det, han selv omtalte som en russisk diplomat. I sin taske havde han bl.a. en liste med navne på nogle af sine studerende.

I årene før anholdelsen mødtes han gentagne gange med russerne. Her udleverede han bl.a. referater og samtaler fra forskellige konferencer samt oplysninger om fire forskere fra Center for Militære Studier. Informationer, der kunne være interessante for den russiske efterretningstjeneste FSB. Årligt modtog han omkring 20.000 kroner i kontanter.

Retten idømte i 2012 professoren fem måneders fængsel for spionage.

TRE DANSKE UNIVERSITETER FALDT FOR SPEAR PHISHING

I 2014-2016 blev et stort antal ansatte på universiteter og i andre organisationer verden over udsat for spear phishing. Spear phishing er målrettede, falske e-mails, som skal få modtageren til at åbne et link eller en vedhæftet fil, der fører til, at angriberne får øget adgang til personens computer og netværk.

Cyberangrebet var i Danmark målrettet medarbejdere med specialer inden for bl.a. økonomi, sundhed, kemi, fysik, geologi, miljø og transport. Medarbejdere fra tre danske universiteter blev narret, og det medførte, at hackerne fik fat i deres kodeord. Ifølge officielle udtalelser fra amerikanske myndigheder havde angrebene tilknytning til iranske myndigheder.

Konsekvenserne er store

Det kan få store konsekvenser for Danmark, hvis andre stater får uønsket adgang til jeres forskning. Det kan også skade danske universiteters ry og skabe problemer med fremtidig finansiering, rekruttering og mulighed for samarbejde.

Udenlandsk indblanding og spionage skaber risiko for tab af:

- **TILLID OG OMDØMME**
  Tilliden til jeres forskning risikerer at forsvinde, hvis de beskyttelsesværdige data, I har adgang til, bliver stjålet eller misbrugt.

- **MULIGHEDER**
  Muligheden for at blive krediteret for jeres arbejde eller for at offentliggøre forskning begrænses, hvis der er sket tab af forskningsresultater.

- **FRIHED**
  Økonomisk afhængighed skaber risiko for økonomisk pression. Direkte eller indirekte trusler om at trække finansieringen til et projekt kan lægge pres på for at gå på kompromis med den akademiske frihed eller formidlings- og ytringsfriheden.

- **FINANSIERING**
  Fremtidig finansiering besværliggøres, hvis det rygtes, at jeres forskning er blevet stjålet af en fremmed stat. I kan ligeledes lide økonomisk tab, hvis nogen får adgang til data eller informationer, der ejes af jeres finansieringskilder.

Udsatte forskningsområder

I takt med den globale udvikling sker der konstant en udvikling i, hvilke forskningsområder der er særligt udsatte. PET kan dog konstatere, at fremmede staters efterretningsvirksomhed kontinuerligt har fokus på de højteknologiske og forsvarspolitiske områder. Alle universiteter herunder en del studieretninger inden for både natur- og samfundsvidenskab samt humaniora er dog potentielt i risiko for udenlandsk indblanding.

Udenlandsk indblanding og spionage mod dansk forskning kan både være kommercielt og politisk motiveret. Stater kan søge at opnå konkurrencemæssig og kommerciel fordel ved at kende til forskernes arbejde og danske forskningsresultater, før de offentliggøres. På områder, der har særligt politisk fokus, kan fremmede stater få indsigt i den forskning og rådgivning, som regeringen og Folketinget baserer vigtige beslutninger på.

FINDES FORSKNINGSINSTITUTTET?

Forskere fra Aalborg Universitet samarbejdede i 2015 og 2016 med en kinesisk ph.d.-studerende, som udgav forskningsartikler sammen med en ingeniør fra Zhengzhou Institute of Information Science and Technology, Zisti.

Problemet er, at forskningsinstituttet tilsyneladende ikke findes, men bruges som dæknavn for det kinesiske militæruniversitet PLA Information Engineering University, der er specialiseret i signalefterretning og udvikling af forsvarsteknologi. Den kinesiske ph.d.-studerende fik viden om avanceret signalteknologi, der kan optimere trådløse signaler i 5G-mobilnetværk, satellit- og radarsystemer. En teknologi, som både kan bruges civilt og militært.

UDVIKLEDE DE MASSEØDELÆGGELSESVÅBEN?

I foråret 2019 slog ledelsen på Institut for Maskinteknik og Produktion på Trondheims universitet NTNU alarm. Uvedkommende havde haft adgang til universitetets database, og PST, den norske efterretningstjeneste, iværksatte en efterforskning. To forskere, som oprindelig er fra Iran, blev i starten af 2020 sigtet for at give uvedkommende adgang til datasystemet. Da databruddet fandt sted, havde forskerduoen en gruppe gæsteforskere fra Iran på besøg. Spørgsmålet er, om forskningen på instituttet kunne bidrage til fremstillingen af masseødelæggelsesvåben. Forskerne blev suspenderet, og sagen efterforskes fortsat.

Hvor udsatte er I?

I bør overveje, hvor udsat jeres forskning er for udenlandsk indblanding og spionage. I de fleste tilfælde er det jer som forskere, der kan vurdere den potentielle interesse og de bredere anvendelsesmuligheder af et forskningsprojekt.

Forskning kan være udsat, hvis:

- Det er sandsynligt, at forskningen fører til et fremtidig kommercielt eller patenterbart resultat.
- Der anvendes følsomme data eller personligt identificerbare oplysninger som fx genetiske oplysninger eller kommercielle testdata.
- Den kan være anvendelig for udenlandsk militær, eller den både kan have militære- og civile anvendelsesmuligheder (dual-use).
- Den potentielt danner grundlag for internationale strategiske politiske forhandlinger eller beslutninger.
- Der benyttes sensitivt laboratorieudstyr.

Sådan får de fingre i jeres forskning

Fremmede stater gør brug af mange forskellige metoder til at indhente oplysninger. Metoder, der strækker sig i et kontinuum mellem lovligt og ulovligt med en del, der ligger i en problematisk gråzone. Typisk benyttes metoderne i et komplekst samspil.

Traditionelt akademisk engagement er en af mange måder, en udenlandsk efterretningstjeneste kan få adgang til jer. Det kan fx foregå ved at udvise interesse for jeres forskning på internationale konferencer eller sociale medier som fx LinkedIn. Et fare-signal kan være, hvis nogen interesserer sig mere for, hvad I *ved*, end hvad I *kan*.

Internationalt samarbejde giver statslige aktører mulighed for at indhente forskning uden at benytte sig af traditionel spionage eller cyberangreb. Samarbejdet kan give uønsket adgang til mennesker, it-netværk og deltagelse i forskning, der kan være beskyttelsesværdig.

METODER TIL UDENLANDSK INDBLANDING OG SPIONAGE

Særligt når det gælder indblanding, kan metoderne være legale, men de kan have et problematisk potentiale, som man bør være opmærksom på.

Menneskerettede metoder

- Rekruttering af studerende og undervisere til udlandet for dermed at indhente viden
- Hvervning af studerende og undervisere, fx til spionage
- Elicitering, dvs. at lokke informationer ud af en person gennem psykologisk manipulering. Oftest vil målpersonen være uvidende om, at elicitering har fundet sted.
- Afpresning, trusler og tvang

Økonomiske metoder

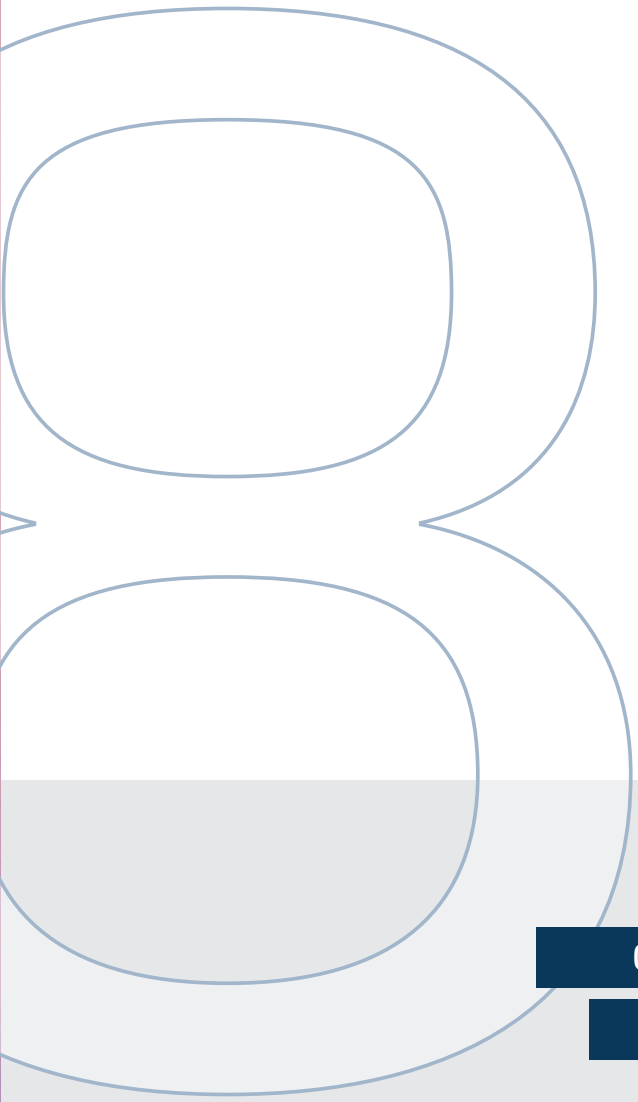
- Legater og tilskud, som kan indeholde problematiske krav eller medføre selvcensur
- Tilbageholdelse af midler eller trussel herom
- Bestikkelse

Digitale metoder

- Informationssøgning på åbne medier, som fx kan danne grundlag for elicitering
- Påvirkningskampagner for at skabe en holdningsændring, fx over for en fremmed stat
- Cyberangreb

Fysiske metoder

- Overvågning
- Tyveri og indbrud



Otte ting I kan gøre for at sikre jer >>

Der er en række ting, I kan gøre for at sikre jeres forskning. De otte råd går dels på at forholde jer til trusselsbilledet, forskningsværdier og samarbejdsrelationer, dels på at opretholde eller indføre tiltag, der kan forbedre sikkerheden. Får I mistanke om, at der foregår noget problematisk, eller er skaden allerede sket, er det desuden vigtigt, at I indberetter det. På den måde kan PET bedre levere konkret, kvalificeret og opdateret rådgivning.

1. Vær bevidste om truslen

En forudsætning for at beskytte jeres forskning er, at I er bevidste om truslen og metoderne til spionage og anden udenlandsk indblanding. I kan dermed holde trusselsbilledet op imod de værdier, fx data og teknologier, som I vurderer, I bør beskytte – se næste punkt. På den baggrund kan I sikre, at jeres sikkerhedsprocedurer og -tiltag er på det ønskede niveau.

Det er desuden vigtigt at udbrede kendskabet til truslen fra indblanding og spionage, så der er konsensus om at gøre en fælles indsats.

2. Vurder værdien af jeres forskning

Det er forskerne selv, der er de bedste til at vurdere værdien og anvendelsesmuligheder af et forskningsprojekt. Den ansvarlige forsker bør derfor overveje, om forskningsresultater er kommercielt interessante, er relateret til sikkerheds- og forsvarsteknologier, har både civile og militære anvendelsesmuligheder m.m. – se afsnittene "Udsatte forskningsområder" og "Hvor udsatte er I", s. 6-7.

Helt enkelt kan man sige, at I skal overveje, hvilke informationer og data I ikke har "råd" til at miste. Beslut jer for, hvem der skal have adgang til hvad. Giv fx kun adgang til relevante databaser og systemer i forbindelse med datadeling i internationale samarbejder.

3. Sæt rammer for udenlandske besøg

Der kan opstå forskellige problematiske situationer i forbindelse med besøg fra udlandet. Inden besøget kan I vurdere, hvilke informationer, I gerne vil dele med jeres gæster, og særligt hvad I ikke ønsker at dele. Vær opmærksomme på, hvis der foretages ændringer i deltagerlisten i sidste øjeblik. Gå lokalerne igennem inden besøget, så der ikke ligger beskyttelsesværdige informationer fremme, der hvor de besøgende får adgang.

Under besøget kan I være opmærksomme på, om gæsternes adfærd afviger fra normalbilledet. Fotograferer og filmer de atypisk meget? Er der deltagere, der ikke holder sig til gruppen, men forsvinder og dukker op uventede steder? Bliver der stillet spørgsmål, som falder uden for besøgets formål? Tillad ikke, at fremmed software og hardware bliver installeret – heller ikke i forbindelse med præsentationer. Det er bedre, hvis de besøgende kobler deres egen computer til en projektor frem for at benytte et USB-stik i jeres computer. For at undgå kritiske situationer bør I bl.a. sørge for et tilstrækkeligt antal medarbejdere, der kan ledsage gæsterne og holde opsyn.

I er meget velkomne til at orientere PET på forhånd, hvis I får besøg, der har national sikkerhedsinteresse ud fra delegationens sammensætning og besøgets formål.

4. Vær forsigtig på rejser

Det er værd at være sikkerhedsmæssigt godt klædt på til rejseaktivitet, konferencer og udlandsophold. For i udlandet er I generelt mere udsatte for tyveri, cybertrusler m.m. Derfor bør I inden afrejse vurdere, hvor mange beskyttelsesværdige informationer, I har behov for at medbringe – og naturligvis have en backup. Det kan også være en god ide at udfærdige en liste over, hvilke dokumenter og data I medbringer. På den måde kan I have et overblik over, hvilken information der kan være blevet tilgået af uvedkommende.

Vær opmærksom, hvis I "tilfældigt" støder ind i mennesker, som udviser ekstra interesse for jeres arbejde eller for jer som privatpersoner. Det kan være en måde, en udenlandsk efterretningstjeneste forsøger at indhente oplysninger på. Bor I på hotel, skal I være opmærksomme på, at personale m.fl. med al sandsynlighed godt kan tilgå værdiboksen.

Wi-fi i udlandet kan være overvåget, så I bør ikke tilgå beskyttelsesværdigt materiale via denne forbindelse. Brug derfor en VPN-tjeneste. Hav jeres udstyr under opsyn, lån det ikke ud, og benyt ikke fremmed udstyr. Slå også gerne Bluetooth fra på alle jeres enheder. På konferencer er det meget normalt at få udleveret USB-stik.

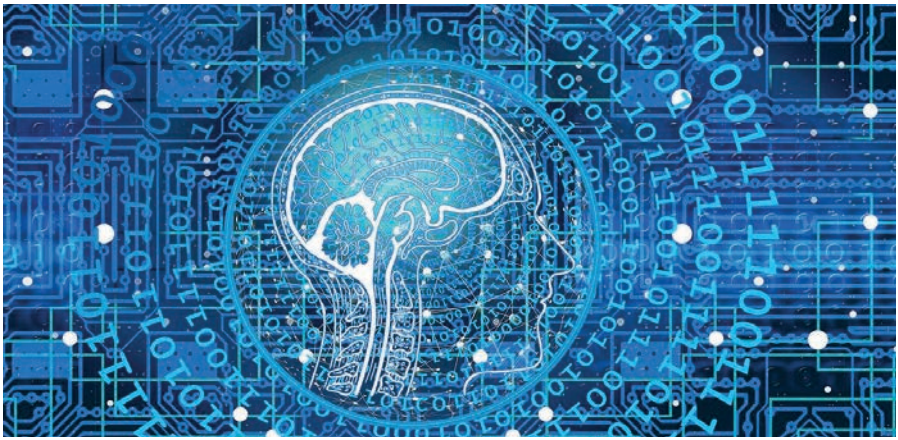
Vær opmærksom på, at de kan indeholde malware – se næste råd om IT-sikkerhed.

Det optimale er at medbringe låneudstyr på rejsen. Alternativt kan det være en ide at slette så meget som praktisk muligt, fx opkaldshistorik, beskeder etc. fra eget udstyr. Når du er hjemme igen, kan du vælge at udskifte dine kodeord til de tjenester, som du har brugt under rejsen.

Se i øvrigt folderen "IT-sikkerhed på rejsen", som er udgivet af Center for Cybersikkerhed.

ET GODT TILBUD VIA LINKEDIN

En dansk sikkerhedspolitisk ekspert modtog en henvendelse via LinkedIn fra en kinesisk kvinde, som tilsyneladende arbejdede for et headhuntingsfirma. I forbindelse med forskerens besøg i Kina i 2012 aftalte de at mødes på et hotel i Beijing. Men kvinden dukkede aldrig op. I stedet førte en ung mand den danske forsker ind i et konferencerum, hvor tre midaldrende mænd befandt sig. De fortalte, at de arbejdede for et regeringsstyret forskningsinstitut, og de havde et tilbud: Forskeren kunne få finansieret sin forskning – til gengæld for at arbejde for dem. Samarbejdet kom dog aldrig i stand, da forskeren ved hjemkomst meldte episoden til myndighederne.



5. Hav fokus på jeres IT-sikkerhed

Når det kommer til IT-sikkerhed, er der dels den tekniske, dels den menneskelige side af sagen. Teknisk set er der forskellige procedurer og tiltag, der kan forbedre sikkerhedsniveauet, inkl. en installering af en effektiv sikkerhedspakke med bl.a. antivirusprogram og spamfilter samt adgang via en VPN-forbindelse. Alt IT-udstyr bør opdateres jævnligt, så det har de nyeste sikkerhedsopdateringer.

Hertil kommer så den menneskelige adfærd. Du er bedre beskyttet, hvis:

- Du opdeler dit arbejdsliv og privatliv, så du ikke bruger din private e-mailadresse og mobiltelefon i arbejdsregi. For alt udstyr gælder det, at du bør låse skærmen, når du forlader den, så et øjebliks uopmærksomhed ikke kan betyde, at uvedkommende får adgang.
- Du tjekker dine privatlivsindstillinger på de sociale medier og overvejer, hvilke personlige informationer du lægger ud. Oplysninger fra sociale medier vil bl.a. kunne blive brugt imod dig eller dine kolleger til spear phishing.
- Du aldrig klikker på vedhæftede dokumenter eller links, som du ikke er sikker på kommer fra en troværdig kilde.
- Du ikke benytter brugte USB-stik, medmindre du stoler på personen eller firmaet, de kommer fra. USB-stik kan indeholde malware, så det bliver muligt at tilgå din computer.
- For yderligere råd om IT-sikkerhed kan du med fordel besøge www.cfcs.dk og www.sikkerdigital.dk. Se desuden publikationen "Råd om sikkerhed på mobile enheder", som er udgivet af Center for Cybersikkerhed og PET.

6. Hav fokus på jeres fysiske sikring

I kan arbejde med den fysiske sikring for at reducere risikoen for tyveri af viden, teknologi og produkter. Mange tiltag skal realiseres centralt. Det gælder fx valg af adgangskontrol, alarmer og overvågning.

Men den enkelte kan også gøre en forskel:

- Har I adgangskoder, så beskyt dem, så uvedkommende ikke kan aflæse dem.
- Vær opmærksom på detaljerne i det fysiske miljø – er der fx tegn på, at der har været forsøg på indbrud?
- Begræns mulighederne for indkig udefra. Indret din arbejdsplads så skærme, tavler mv. vender væk fra fx vinduer. Alternativt kan I bruge gardiner og persienner efter behov.
- Brug lokalerne, som de er planlagt. Flyt fx ikke en mødedrøftelse fra mødelokalet til tekøkkenet.
- Vær bevidst om synlige sårbarheder som fx åbne vinduer i stueetagen.
- Vær opmærksom på kompromittering af fysiske sikringsforanstaltninger som fx kiler i sikringsdøre.
- Etabler og overhold en procedure for sikker opbevaring. Har I et skab med kode, bør I sikre, at den ikke kan blive aflæst.
- Etabler og overhold en lukkeprocedure, så fx vinduer, døre og skabe lukkes, når lokalet forlades.
- Etabler og overhold en politik for sikker bortskaffelse af dokumenter og lignende. Brug fx en makulator.
- Bær dit ID-kort synligt inden for den fysiske sikring. Det reducerer bl.a. muligheden for "tail-gating" – at en person uden ID-kort hægter sig på en, der har det, og på den måde skaffer sig uautoriseret adgang. Gem dit ID-kort væk, når det ikke er relevant længere, fx til og fra din arbejdsplads.

7. Pas på jer selv – især når I er sårbare

De udenlandske efterretningstjenester, der arbejder med indblanding og spionage, har typisk indgående kendskab til menneskets psykologiske behov og tilbøjeligheder. Det kan de udnytte til at forsøge at få jer til at åbne filer eller sende loginoplysninger og at dele flere personlige data, end I har lyst til.

Vores naturlige tilbøjelighed til at have tillid til andre samt ønsket om bekræftelse og anerkendelse, kan blive brugt imod en. Risikoen vil i den forbindelse være øget, hvis man har faglige eller personlige frustrationer. Er man i en ekstra sårbar position, fx pga. gæld, utroskab, misbrug eller kriminalitet, vil det desuden kunne bruges til bestikkelse eller afpresning.

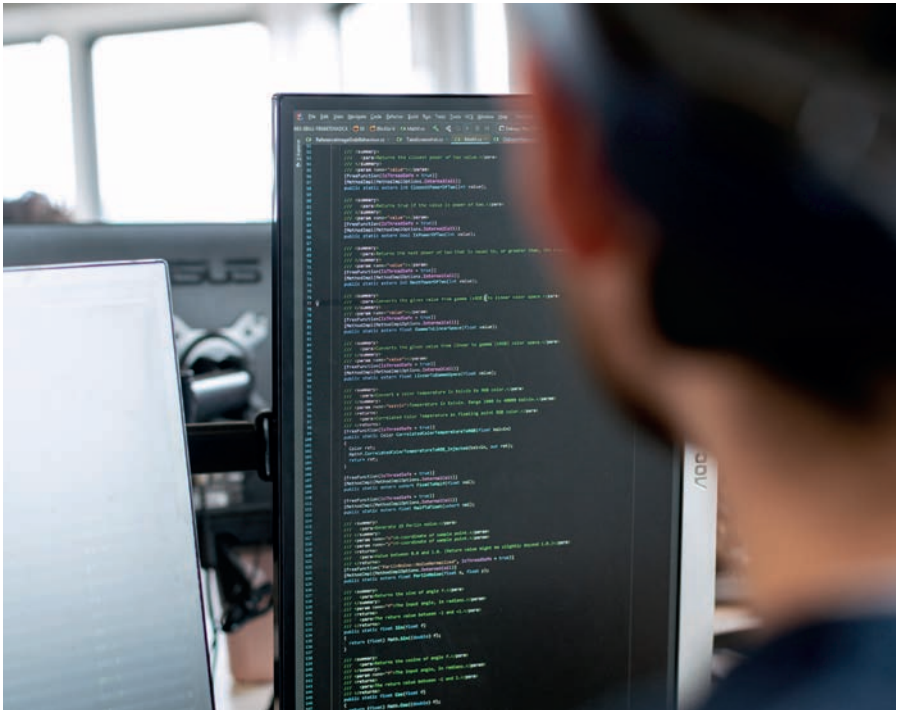
8. Sig noget, hvis I ser noget

– Har I en bekymring, eller er skaden sket?

Hvis I oplever noget, som giver anledning til bekymring, i forhold til udenlandsk indblanding eller spionage, bør I indberette det. Alt efter jeres institutions organisering kan I melde jeres bekymring eller mistanke til nærmeste chef, til ledelsen, den sikkerhedsansvarlige, Uddannelses- og Forskningsministeriet eller direkte til PET.

Det kan fx dreje sig om mistænkelig opførsel hos en samarbejdspartner eller en besøgende. Det kan også være, I har mistanke om overvågning. PET kan levere konkret rådgivning i forhold til implementering af eventuelle forebyggende og sikkerhedsmæssige foranstaltninger eller procedurer. I henvender jer til PET via pet@politi.dk, hvor I enten kan anmode om et møde eller sende en skriftlig beskrivelse af jeres bekymring eller observation.

Er hændelsen cyberrelateret, bør I kontakte Center for Cybersikkerhed, CFCS, samt PET. Se "Kontakt" s. 19.



Otte ting, I kan gøre for at sikre jer

1. Vær bevidst om truslen
2. Vurder værdien af jeres forskning
3. Sæt rammer for udenlandske besøg
4. Vær forsigtig på rejser
5. Hav fokus på IT-sikkerhed
6. Hav fokus på fysisk sikring
7. Pas på jer selv – især når I er sårbare
8. Sig noget, hvis I ser noget

Kontakt

POLITIETS EFTERRETNINGSTJENESTE
Klausdalsbrovej 1
2860 Søborg
Tlf. 45 15 90 07
E-mail: pet@politi.dk
www.pet.dk

CENTER FOR CYBERSIKKERHED
FORSVARETS EFTERRETNINGSTJENESTE
Postadresse: Kastellet 30
Besøgsadresse: Holsteinsgade 63
2100 København Ø
Tlf. 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

UDDANNELSES- OG FORSKNINGSMINISTERIET
Postadresse: Postboks 2135
Besøgsadresse: Børsgade 4
1215 København
Tlf. 35 44 62 00
E-mail: ufm@ufm.dk
www.ufm.dk

© Politiets Efterretningstjeneste
Udgivet: Maj 2021
Tryk: AtlasGrafisk
Grafisk design: Designlinjen.dk

Uddannelses- og Forskningsministeriet

PEET