DKCERT

DeiC

DeiC-konferencen 2023:
Truslen fra den menneskerlige faktor

DKCERT
www.cert.dk
Eskil Sørensen
Email: eskil.sorensen@deic.dk

> Lidt fakta

> Cand.comm
> Sikkerhedskonsulent, sikkerhedsformidler DKCERT 2020-
> Digitaliseringsstyrelsen 2011-2019
> It- og Telestyrelsen 2005-2011

> Mine interesseområder:
> Hvordan vi kan formidle cybersikkerhed uden at vi taler henover hovedet på folk, så det får en sikkerhedsmæssig effekt?

> **Der**

> 80 p

> 90 p

> 81%
infor
risik

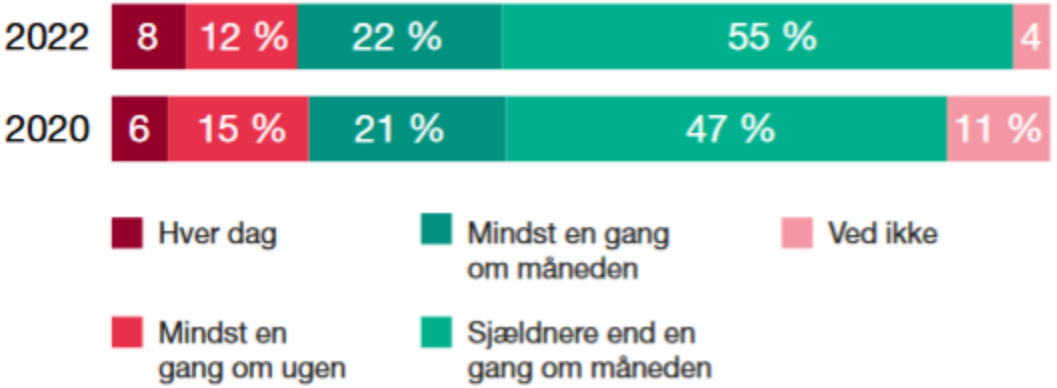
> Det g
eller

fejl.

ne på

ning

Hvor ofte undlader du at efterleve informations-sikkerhedspolitikkerne og/eller -retningslinjerne for din arbejdsplads?



Anm.: n = 141 (2022) og 157 (2020).

> Den uagtsomme medarbejder

> Har kendskab til eller er uddannet i organisationens sikkerhedspolitik

> Vælger at omgå dem for at være mere effektiv, eller hvis politikkerne ses som besværlige.

> Mest sårbar over for sjusk

> Den ubevidste medarbejder

- > Uvidende om organisationens sikkerhedspolitik
- > Forstår de potentielle sikkerhedsrisici
- > Skænker ikke skænker sikkerhed en tanke.

- > Mest sårbare over for social engineering

> Den uvederhæftige medarbejder

> Stjæler data med vilje
> Ødelægger virksomhedsnetværk
> Sletter virksomhedsdata

> Kan være god til at slette sine spor

Håndteringen af truslen fra den menneskelige faktor på AAU

Michael Collin

8. November 2023

AALBORG UNIVERSITET

Håndteringen af truslen fra den menneskelige faktor på AAU

Truslen er blevet adresseret løbende

- Generelt er den løbende awareness-træning del af håndteringen af truslen fra den uagtsomme og den ubevidste medarbejder
- Vi arbejder løbende på at få vurdering af risici til at komme mere i øjenhøjde for forskerne og derved håndtere truslen fra de uagtsomme og de uvederhæftige medarbejdere
- Da pressen har hetz mod TicToc opstod der ønske fra ledensen om at stramme på regler og adressere truslen fra den ubeviste og den uvederhæftige medarbejder
- Da PET besøgte universitetsledelserne og URIS-rapport forelå opstod der ønske om at stramme processer for besøg og ansættelser af videnskabelige medarbejdere.

Kilde: DKCERT trendrapport 2022

Beskyttelse mod uønsket software

Informationssikkerhedsudvalg beslutning:

ITS skal vedligeholde en liste over uønsket software på devices, som indeholder AAU-data

Efter dialog med SDU, som er meget restriktiv, har vi udarbejdet følgende, som vi **påtænker** at sætte på listen over uønsket software (Pt. målrettet Windows):

- Software der ændrer opsætningen på enheden eller i programmerne. (Bl.a. QQ- og torrent-programmer)
- Gratis Software, som ikke er gratis til virksomhedsbrug (Det kommer ofte i en Bundlet pakke, som kan indeholde "overraskelser" (Tilføjer ny browser, søgemaskine, anti-virus m.m.))
- Sikkerhedsapplikationer som ikke er AAU styrede-/leverede (Antivirus-/ Anti-malwareprogrammer).
- VPN-software som ikke er AAU styrede-/leverede.
- Software der åbner op for angrebsflader udenom AAU egne "leveringsløsninger". F.eks. WeChat, Facebook Messenger, TikTok, Chat apps og lign.
- Internetbrowsere udover dem, som ITS indstallerer (AAU installerer: Edge Chromium, Internet Explorer, Firefox ESR, Google Chrome Enterprise.
- Spil som installerer antipirat software
- Alt hvad der ændrer adfærd pga. høstet certifikater eller software komponenter som opfører sig anderledes.

URIS' nye retningslinjer

Ni retningslinjer **under** ***tre overordnede temaer*** **for, hvordan danske institutioner kan øge opmærksomheden samt opbygge strukturer og procedurer, der kan hjælpe ansatte og studerende til at navigere i det komplekse område.**

Retningslinjerne er målrettet ledelserne på uddannelses- og forskningsinstitutionerne og er udarbejdet med henblik på offentliggørelse.

Tema 1

Identificer og beskyt jeres kritiske forskning

Tema 2

Kend jeres samarbejdspartnere

Tema 3

Beskyt jeres institution, ansatte og studerende

Hvorfor nye tiltag?

- URIS: så åbent som mulig og så lukket som nødvendig
- Få styr på hvem vi lukker ind og tage kvalificeret stilling til risici
- Afklare hvad vi har i huset samt krav om tilstrækkelig sikkerhed
- Øge bevidsthed om risiko for industrispionage, misbrug af teknologi og tyveri af resultater
- Løfte institutionsansvar ift. at støtte individets muligheder for at identificere, håndtere og reducere risici
- Bidrage til at AAU og AAU's ansatte ikke uforvarende begår lovbrud eller kommer galt afsted
- Sikre gennemsigtighed i samarbejdet med omverdenen
- Bidrage til at AAU vurderes som en attraktiv og professionel samarbejdspartner

Hvad er eksportkontrol?

EU regler og US regler

Farlige produkter og teknologier, som også kan bruges til at fremstille masseødelæggelsesvåben eller fremføringsmidler

Skal forhindre at konkrollerede produkter og teknologi ikke falder i forkerte hænder

Sanktioner har betydning for hvad du må eksportere til hvem

Lande der er omfattet af sanktioner: Iran, Krim & Servastopol, Nordkorea, Rusland og Syrien

Overførsel af viden og teknologi, som AAU bringer ud af landet som led i samarbejde med eksterne samarbejdspartnere

Viden og teknologi, der overføres i Danmark er omfattet – teknisk bistand

Tiltag

Processer og procedurer – risikovurdering af personer

- Rekruttering af medarbejdere fra enkelte lande TECH og ENG: hvilke institutioner kommer de fra, hvad skal de arbejde med, hvad har de adgang til?
- Modtagelse af gæsteforskere fra enkelte lande; hvilke institutioner kommer de fra, hvad skal de arbejde med, hvad har de adgang til?
- Indskrivning i ph.d.-skole: hvilke institutioner kommer de fra, hvad skal de arbejde med, hvad har de adgang til?

Hvordan risikovurdere?

- Formål: at afdække hvem der har adgang til hvad
- Risikovurdering foretages på baggrund af offentligt tilgængelige oplysninger
- Best effort
- Kan anmode om kundetjek hos Erhvervsstyrelsen – findes der kritiske oplysninger om hjemuniversitetet?
- Hvilke lande? Personer fra de lande som PET peger på i deres vurdering af trusselsbilledet – inklusiv lande som er sanktioneret af EU, herunder Rusland, Hviderusland og Iran
- URIS arbejdsgruppen har en repræsentant fra hver af de danske universiteter - deler værktøjer til screening imellem sig – AAUs screeningsværktøjer er delt med de øvrige danske universiteter
- Yderligere spørgsmål til AAUs procedure kan rettes til Ulla Olesen ukp@adm.aau.dk

Risikovurderingens indhold

- Baggrundstjek af personens historik; emner for tidligere publikationer, tilknytning/forskergruppe/vejleder
- Baggrundtjek af hjeminstitutionens/virksomhedens profil: ASPI-liste, relevante slutbrugerlister eksempelvis US Entity list, renommé: kendt for hvad?
- Finansiering - hvor kommer pengene fra?
- Hvem har foreslået emnet?
- Overvejelser om emnets potentielle politiske og etiske problemstillinger, mulige anvendelser.
- Omhandler eller anvender projektet kritisk teknologi (dual-use, kritisk infrastruktur og lign.)?
- Vurdering af om personen får adgang til kritisk teknologi, udstyr, data og informationer.
- Kan forskningen anvendes til militære formål? – overvej risiko for direkte eller indirekte at støtte opbygning af militære kapaciteter i de pågældende lande

Screeningsprocedurer
Gæster/ansættelse

- Projektleder på instituttet udfylder risikovurderingsskema
- Institutleder indhenter udtalelse/bemærkninger om risici fra Kontraktenheden
- Institutleder sender indstilling til dekanen sammen med risikovurderingsskemaet og udtalelse fra Kontraktenheden
- Dekanen kan anmode om yderligere information/udtalelse fra instituttet på baggrund af Kontraktenhedens udtalelse/bemærkninger
- Dekanen træffer beslutning
- Herefter igangsættes invitation til ophold/ansættelsesproces evt.

Screeningsprocedurer
Ph.d.

- Vejleder udfylder risikovurderingsskema i forbindelse med indskrivningsprocessen
- Risikovurderingsskemaet underskrives af vejleder og institutleder
- Risikovurderingsskemaet fremsendes til ph.d.-skolen som indhenter udtalelse/bemærkninger om risici fra Kontraktenheden
- Udtalelse/bemærkninger fra Kontraktenheden kan indeholde yderligere baggrundstjek af hjeminstitution/tidligere arbejdsgiver)
- Ph.d.-skoleleder bekræfter indstilling om indskrivning med underskrift på risikovurderingsskemaet
- Dekanen træffer beslutning
- Herefter igangsættes indskrivningsproces evt.

Spørgsmål?