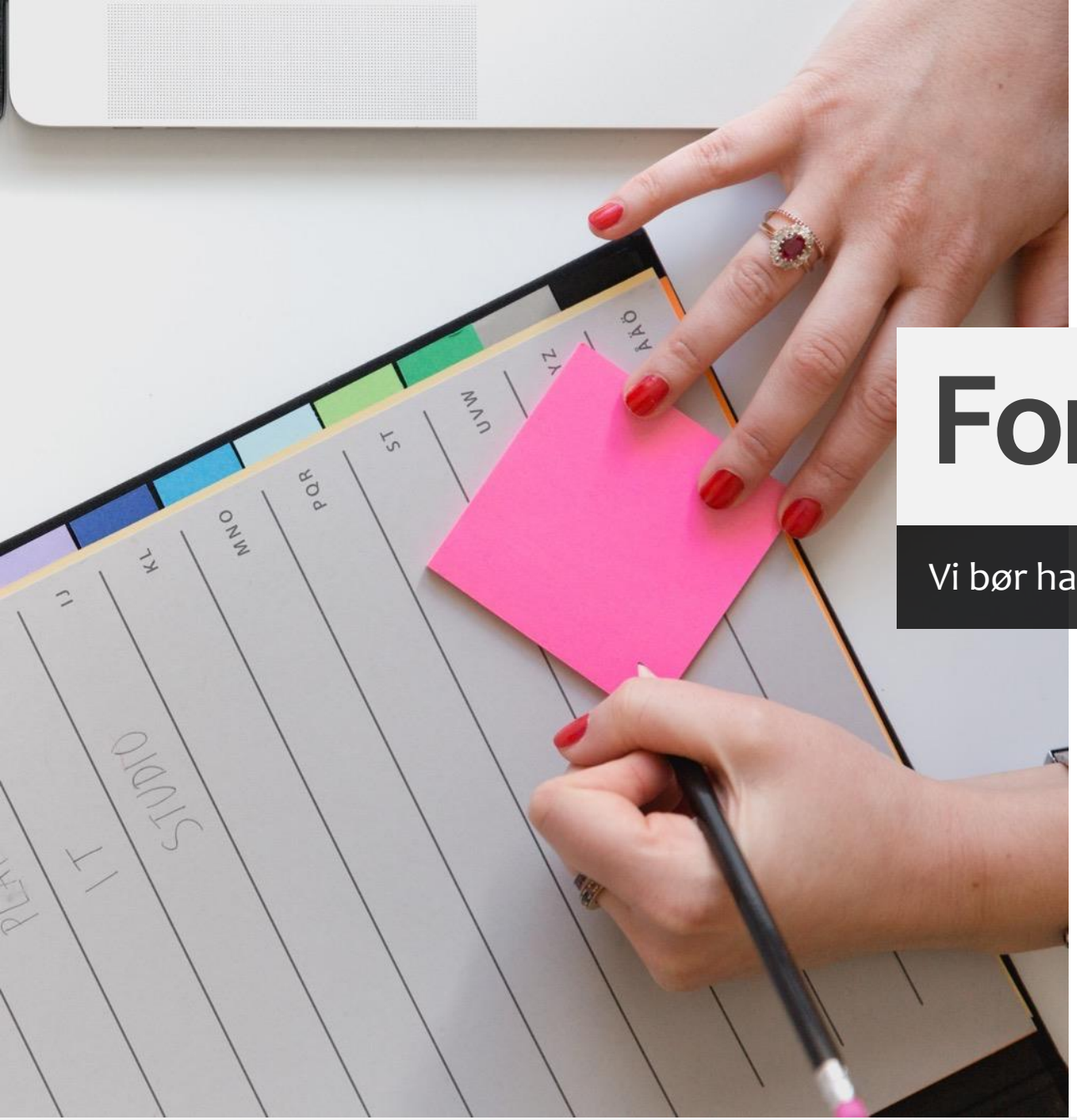
Beredskabsplan

FGU Danmark

Ingen lovkrav til beredskabsplan

- Men, det gør krisestyring lettere
- Men, det skaber overblik
- Men, det giver ro i maven



Formål

Vi bør have en beredskabsplan fordi

- Den bidrager til en stabil og sikker drift,
- Den minimerer/ forhindrer tab af data
- Den giver medarbejderne mulighed for at handle hurtigt og præcist i tilfælde af et angreb.

Kriseorganisation

Hvem har ansvaret

Kriseorganisation

I tilfælde af en krisesituation som følge af hackerangreb, sabotage eller tilsvarende

Hvem skal kontakte hvem

- Umiddelbart efter du erkender at et angreb, et sikkerhedsbrud, et systemnedbrud eller en sabotageaktivitet har ramt dit driftsmiljø, skal du omgående kontakte nærmeste leder eller den IT-ansvarlige og informere om, hvad du har erkendt.

Kriseorganisationen

- Kan f.eks. bestå af
- Direktør/rektor
- IT-ansvarlige
- Administrationschef

Det skal være almindeligt kendt, hvem kriseorganisationen består af og hvordan de kan kontaktes

Handleplan

I tilfælde af en krisesituation som følge af hackerangreb, sabotage eller tilsvarende

Hvem skal uføre hvilke opgaver

- Umiddelbart efter at være adviseret om problemet skal den IT-ansvarlige eller den pågældende leder kontakte Support-desk hos Statens IT eller anden driftsleverandør og informere om den indtrufne hændelse:

Informations flow

- Hvad har man oplevet
- Hvornår er hændelsen første gang konstateret
- Hvem er FGU XX kontaktperson for yderligere informationer.

Vigtigt:

Bestyrelse og ledelsen skal give krisestaben arbejdsro og vise tillid til at de kan løse opgaven.
Utidig indblanding vil ikke bidrage positivt til opgavens løsning!

Opfølgning på beredskabet

I tilfælde af en krisesituation som følge af hackerangreb, sabotage eller tilsvarende

Dokumentation af hændelse

- Umiddelbart efter anmeldelse af hændelsen til supporten, påbegyndes dokumentation af sagen i en logfil (evt. gerne samme logfil som benyttes til GDPR sikkerhedsbrud).
- Dokumentationen skal i givet fald komme fra udbyderen af den angrebne service. Hvis der f.eks. er tale om et angreb mod det studieadministrative system (IST, FGU Planer), eller hvis det er tale om at hjemmesiden er angrebet, hvorfor det i så fald er den pågældende udbyder f.eks. One.Com.
- Dokumentationen skal indeholdende en beskrivelse af hændelsesforløbet, hvilke foranstaltninger har man truffet til afværgning for at stoppe angrebet. Hvilke foranstaltninger er der truffet for at undgå tilsvarende fremtidige angreb.

Konsekvensvurdering

I tilfælde af en krisesituation som følge af hackerangreb, sabotage eller tilsvarende

- Den dataansvarliges IT-ansvarlige og FGU XX's ledelse skal efterfølgende udføre konsekvensvurdering og evt underretning til berørte personer om evt personlige konsekvenser

- Konsekvensvurdering skal omfatte:
  - Har der været tale om tab af data?
  - Har der været tale om tab af integritet?
  - Har der været tale om tab af tilgængelighed til data og i givet fald, hvor længe?
  - Har der været tale om sabotage af bygningsinfrastruktur eller anden ikke IT-relateret påvirkning.
  - Hvilken konsekvens vurderes hændelsen at have haft for FGU XX?
  - Hvilken konsekvens vurderes hændelsen at have haft for de registrerede?
    - Har konsekvensen en karakter, der gør det nødvendigt at informere de registrerede herom?
  - Har konsekvensen en karakter der nødvendiggør anmeldelse til Datatilsynet?
    - Tag kontakt til FGU Danmark fælles DPO for en evt afklaring.
  - Har konsekvensen en karakter der nødvendiggør iværksætning af yderligere fysiske sikkerhedsforanstaltninger?
  - På baggrund af de trufne foranstaltninger, hvor sandsynligt vurderes det, at denne type hændelse kan genopstå?

Spørgsmål?