Testscenarier

**Indholdsfortegnelse**

[Anvendelse af testscenarier 2](#_Toc106873504)

[Testscenarie 1 - Hackerangreb 3](#_Toc106873505)

[Testscenarie 2 - Strømafbrydelse 5](#_Toc106873506)

[Testscenarie 3 - Systemfejl Bosted 7](#_Toc106873507)

[Testscenarie 4 – Ransomeware angreb 9](#_Toc106873508)

[Testscenarie 5 – WAN problemer 10](#_Toc106873509)

# Anvendelse af testscenarier

Testscenarierne skal betragtes som et idekatalog, der kan bruges som inspiration til test af beredskab for informationssikkerhed.

Scenarierne er bygget op i faser, hvor der er beskrevet indspil for hver fase. Under hver fase står der en række spørgsmål. Spørgsmålene har to formål:

1. Den testansvarlige/projektlederen kan anvende dem som en tjekliste ift. om beredskabet kommer rundt om de forskellige issues. Der kan også improviseres indspil undervejs, hvis nogle af spørgsmålene ikke adresseres.
2. Observatøren kan strukturere observationerne ift. spørgsmålene og adressere områder, som beredskabet eventuelt ikke forholder sig til eller glemmer.

Alle scenarier skal tilpasses lokale forhold og den lokale organisation.

Der kan frit tilføjes og fjernes indspil, som det passer ift. det man ønsker at teste.

# Testscenarie 1 - Hackerangreb

**Alarmering om hændelse**

*Start på Øvelse. Klokken er 10.25*

Brugere melder at det ikke er muligt at tilgå Cura/Nexus fra hjemmeplejens pc – det virker på mobilappen, men der kan ikke trækkes oplysninger om medicin og der kan ikke laves kørelister til hjemmehjælperne.

Kommunens firewall er overbelastet med indgående trafik. Det har stået på i 45 min.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Er det nødvendigt at stoppe adgangen til internettet?
* Hvem skal kontaktes og informeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Afdækning af omfang**

*Klokken er nu 10.50*

Det kan nu afgøres, at system x, y og z ligeledes er utilgængelig.
System W, V og T er upåvirkede.

Via en privat forbindelse ses, at der er angreb fra IP i Rumænien, Hvide Rusland og Estland.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvordan kommunikeres der?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Eskalering**

*Klokken er nu 11.05*

IT-drift indser, at der er et massivt DDOS-angreb på kommunen.

Det kommer frem via et news-feed, at mange kommuner er ramt og at mindst 1 kommune mener at deres sikkerhed er brudt.

Direktionen spørger til tidshorisont og konsekvenser

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvordan kommunikeres der?
* Skal der kommunikeres eksternt?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Normalisering**

*Klokken er nu 12.06*

TDC oplyser at de har spærret for trafikken fra de tre områder.

Belastningen på vores firewall er normal.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvordan kommunikeres der?

# Testscenarie 2 - Strømafbrydelse

**Alarmering om hændelse**

*Start på Øvelse. Klokken er 9.00 og det er fredag*

Lyset går i bygningen, ventilationen stopper, pc'er, printere og skærme slukker overalt.

**Spørgsmål**:

* Hvilke handlinger foretages?
* Hvem skal informeres?
* Hvordan kommunikeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Afdækning af omfang**

*Klokken er nu 9.15*

Der er ikke tale om en lokal strømafbrydelse.
Datacentret er ramt af strømafbrydelse og der er problemer med at få koblet nødgeneratoren til.

De kritiske forretningssystemer er tilsluttet UPS, som er blevet aktiveret automatisk, men den har kun kapacitet til 30 min, hvorefter systemerne automatisk lukker ned.

**Spørgsmål**:

* Hvilke handlinger foretages?
* Hvordan skal der eskaleres?
* Er der forretningsnødplaner, som skal iværksættes?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Videreførelse af forretningen**

*Klokken er nu 9.45*

De kritiske forretningssystemer er nu lukket ned. IP-telefoni er afbrudt og printere er også utilgængelige.

Lederen af den afdeling, der anvender kommunens mest kritiske forretningssystem, er sygemeldt og kan ikke kontaktes.

**Spørgsmål**:

* Hvilke handlinger foretages?
* Hvordan videreføres forretningen?
* Hvordan kommunikeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Kommunikation**

*Klokken er nu 10.00*

Strømafbrydelsen er alvorlig. Forsyningsselskabet forventer at strømmen er tilbage indenfor 4-5 timer.

Nødgenerator kan ikke blive funktionsdygtig, da man mangler reservedele.

**Spørgsmål**:

* Hvordan skal der kommunikeres?
	+ Internt?
	+ Med øvrige eksterne interessenter?
* Hvilke handlinger foretages?
* Hvordan videreføres forretningen i perioden?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Normalisering**

*Klokken er nu 15.30*

Strømmen er kommet tilbage og er meldt stabil. Lyset er tændt igen, pc'ere, skærme og printere virker igen.

Genopstart af systemer kan påbegyndes.

Knud, der kender alt til kommunens it-infrastruktur, servere og sammenhænge mellem forretningssystemer, har desværre været nødt til at gå, da han skulle hente børn.

**Spørgsmål**:

* Hvilke handlinger foretages?
* Er der særlige funktioner eller data, som skal testes?
* Hvordan kommunikeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

# Testscenarie 3 - Systemfejl EG Bosted (eller andet system med integration til FMK)

**Alarmering om hændelse**

*Start på Øvelse. Klokken er 11.00 på en mandag*

En medarbejder meddeler at data i Bosted ser ”mystisk” ud. Data er ændret selvom medarbejderen med sikkerhed ved at ingen andre har været inde og skrive på en given borgers journal siden sidst. Der står nu en helt forkert diagnose på borgeren. Integrationen til FMK er desuden nede.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvem skal informeres?
* Hvordan kommunikeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Afdækning af omfang**

*Klokken er 12.00*

Det konstateres at der er rod i data i stort set alle journaler. Leverandøren kan se at der har været adgang til databasen udefra, og der er kørt et script, som har sorteret 3 af felterne alfabetisk, så data for de tre felter nu står under forkerte CPR-numre. Der er siden fejlen opstod desuden rettet i journalerne manuelt. Det konstateres at FMK ikke er nede, men integrationen fungerer fortsat ikke. Hændelsen er så omfattende at det kommer til at tage minimum 1 døgn at rydde op i. Det vil sandsynligvis være nødvendigt at indlæse backup som nu er 11 timer gammel.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Er der forretningsnødplaner, som skal iværksættes?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Videreførelse af forretningen**

*Klokken er 12.15*

Forretningen skal forberede sig på at der går minimum 1 døgn, inden man igen kan stole på data. Sandsynligvis længere. Det er ukendt hvilken medicin man skal give borgerne. Der er sygdom på et af bostederne, så der er kun en relativt ny medarbejder på arbejde, og resten er vikarer.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvordan videreføres forretningen?
* Hvordan kommunikeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Kommunikation**

*Klokken er 12.30*

Man har konstateret at backup er eneste løsning. Alle brugere skal derfor orienteres om at man ikke må anvende data i løsningen, og at alle opdateringer siden mandag kl. 01.00 er tabt.

**Spørgsmål:**

* Hvordan skal der kommunikeres?
	+ Internt?
	+ Med leverandøren?
	+ Med øvrige eksterne interessenter?
* Hvilke handlinger foretages?
* Hvordan videreføres forretningen i perioden?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Normalisering**

*Det er nu tirsdag. Klokken er 15.30*

Leverandøren har indlæst backup fra mandag nat kl. 01:00

**Spørgsmål:**

* Hvilke handlinger foretages?
* Er der særlige funktioner eller data, som skal testes?
* Hvordan kommunikeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

# Testscenarie 4 – Ransomeware angreb

**Alarmering om hændelse**

*Start på Øvelse. Klokken er 11.15*

3 ansatte melder, at der på deres skærm er en trussel om ransomware.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvem skal kontaktes og informeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Afdækning af omfang**

*Klokken er nu 11.35*

Dele af harddisk ER krypteret med en cryptolocker.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Findes den nødvendige viden i organisationen?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Eskalering**

*Klokken er nu 12.00*

Der er krav om løsepenge for at dekryptere harddiskene. Der er fundet 3 biblioteker, der er krypteret

**Spørgsmål:**

* Hvilke handlinger foretages?
* Findes den nødvendige viden i organisationen?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Normalisering**

*Klokken er nu 16.45*

Der er tilsyneladende ikke andre brugere, der har brugt disse biblioteker. Biblioteker er nu fjernet.
Biblioteker er restoret fra backup.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvordan kommunikeres der?

# Testscenarie 5 – WAN problemer

**Alarmering om hændelse**

*Start på Øvelse. Klokken er 09.45*

Der ringes fra flere institutioner, at der er problemer, hvor systemer er utilgængelige.

Der er lange svar tider mod visse lokationer og ingen forbindelse til andre.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvem skal kontaktes og informeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Afdækning af omfang**

*Klokken er nu 10.10*

WAN leverandøren meddeler, at de oplever periodiske fejl i deres netværk. De er ved at undersøge.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvem skal kontaktes og informeres?

**Eskalering**

*Klokken er nu 10.20*

WAN-leverandøren oplyser, at problemet skyldes en fejlbehæftet opdatering af deres udstyr.
De estimerer, at det vil tage 2 arbejdsdage, at løse problemet. De tilbyder at opstille mobile ”hotspots” som nødløsning. Der vil dog være begrænset båndbredde til rådighed.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Er der overblik over konsekvenserne?
* Hvem skal kontaktes og informeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?

**Videreførsel** **af forretningen**

*Klokken er nu 11.00*

Nødløsning med hotspots kan kun servicere ENTEN trådløse enheder ELLER kablede enheder.

**Spørgsmål:**

* Hvilke handlinger foretages?
* Er der overblik over konsekvenserne?
* Er der styr på prioriteringen af systemer / fysiske lokationer?
* Hvem skal kontaktes og informeres?

**Normalisering**

*To dage senere. Klokken er nu 12.00*

WAN-leverandøren oplyser, at problemet er løst og netværket fungerer igen

**Spørgsmål:**

* Hvilke handlinger foretages?
* Hvem skal kontaktes og informeres?
* Er alle relevante oplysninger at finde i beredskabsplanen?