Dubex:

Cyber Beredskabsplan

SME Template

Virksomhed: [VIRKSOMHEDSNAVN]
Version: 1.0
Dato: [DATO]
Godkendt af: [CEO/IT-ANSVARLIG]
Næste revision: [DATO + 12 MÅNEDER]

---

1. OVERSIGT OG FORMÅL

Formål

Denne plan sikrer, at [VIRKSOMHEDSNAVN] kan reagere hurtigt og effektivt på cyberhændelser for at minimere forretningsmæssig påvirkning og beskytte kundedata.

Hvorfor er dette kritisk? Cyberhændelser kan lukke en virksomhed ned inden for få timer, hvis der ikke er en klar plan for hvordan man reagerer. Statistikker viser at 60% af små og mellemstore virksomheder lukker inden for 6 måneder efter et alvorligt cyberangreb. Dette skyldes ikke kun den tekniske skade, men også tab af kundetillid, juridiske konsekvenser og ødelæggelse af virksomhedens omdømme. Med en solid beredskabsplan kan I reducere nedetid fra dage til timer og bevare både kundeforhold og forretning.

Forretningsmæssig værdi: En velfungerende cyber beredskabsplan fungerer som en forsikringspolice der beskytter jeres investering i virksomheden. Den reducerer ikke kun skaderne når noget går galt, men viser også overfor kunder, leverandører og forsikringsselskaber at I tager cybersikkerhed seriøst. Dette kan give jer konkurrencefordele ved kundeforhandlinger og bedre forsikringsrater.

Anvendelsesområde

- Gælder for: Alle medarbejdere og IT-systemer
- Aktiveres ved: Mistænkelig eller bekræftet cyberhændelse
- Ansvarlig: [IT-ANSVARLIG/NAVN]

Cybersikkerhed er ikke kun IT-afdelingens ansvar. Enhver medarbejder kan være det første link i kæden der opdager en trussel, og enhver kan også utilsigtet være indgangspunktet for et angreb. Derfor skal alle forstå deres rolle i at både forebygge og reagere på cyber-trusler. Dette inkluderer alt fra at genkende mistænkelige emails til at vide hvem de skal kontakte hvis noget virker forkert.

Kritiske Kontakter (Print ud og hæng op!)

Rolle	Navn	Telefon	Email	Backup
IT-Ansvarlig	[NAVN]	[TLF]	[EMAIL]	[BACKUP NAVN]
CEO/Direktør	[NAVN]	[TLF]	[EMAIL]	[BACKUP NAVN]

Rolle	Navn	Telefon	Email	Backup
Ekstern IT-leverandør	[FIRMA]	[TLF]	[EMAIL]	[BACKUP TLF]
Forsikringsselskab	[FIRMA]	[TLF]	[SAGSNR]	[BACKUP]

2. KLASSIFICERING AF HÆNDELSER

Cyberhændelser kommer i mange former og størrelser, og det er afgørende at forstå forskellen for at kunne reagere proportionalt. Ved at klassificere hændelser kan vi sikre, at vi ikke spilder kritiske ressourcer på mindre problemer, mens vi samtidig eskalerer hurtigt nok når noget virkelig alvorligt sker.

Hvorfor er klassificering vigtig? Uden klar klassificering risikerer vi at over-reagere på små problemer (hvilket koster tid og penge) eller under-reagere på store trusler (hvilket kan ødelægge forretningen). Klassificeringen hjælper også med at kommunikere trusselens alvor til ledelsen og bestemme hvilke ressourcer der skal aktiveres.

🟢 NIVEAU 1 - LAV RISIKO

Eksempler: Mistænkelig email, enkelt PC med virus, mindre netværksproblemer

- Responstid: Inden for 2 timer
- Ansvarlig: IT-support
- Eskalering: Kun ved forværring

🟡 NIVEAU 2 - MEDIUM RISIKO

Eksempler: Flere PC'er inficeret, email-server nede, mindre databrud

- Responstid: Inden for 30 minutter
- Ansvarlig: IT-ansvarlig
- Eskalering: Informer ledelse

🔴 NIVEAU 3 - HØJ RISIKO

Eksempler: Ransomware, stort databrud, kritiske systemer nede

- Responstid: Øjeblikkeligt
- Ansvarlig: IT-ansvarlig + ledelse
- Eskalering: Aktiver fuldt beredskab

3. RESPONS-TEAM (Skalerbart)

Effektiv krisehåndtering kræver klare roller og ansvarsområder. Tænk på det som et brandværns struktur - alle ved præcis hvad deres job er, så der ikke opstår forvirring eller overlap når sekunderne tæller. I cybersikkerhedsverdenen er det samme princip afgørende for at kunne reagere hurtigt og koordineret.

Under en krise er der en naturlig tendens til at alle vil hjælpe, hvilket kan føre til kaos hvis ikke der er en klar kommandostruktur. Samtidig kan kritiske opgaver blive overset hvis alle antager at "nogen andre" tager sig af dem. Ved at definere hvem der gør hvad på forhånd, undgår I både forvirring og ineffektivitet når I mindst kan bruge det.

Basis Setup

- Incident Commander: IT-ansvarlig
- Teknisk ansvarlig: IT-support/ekstern leverandør
- Kommunikationsansvarlig: Administrationschef/CEO
- Beslutningsansvarlig: CEO

Udvidet Setup

- Incident Commander: IT-manager
- Teknisk team: IT-ansvarlig + IT-support + ekstern
- Kommunikationsteam: HR-chef + Kommunikationsansvarlig
- Beslutningsgruppe: CEO + Driftschef + IT-manager
- Dokumentationsansvarlig: Administrativ medarbejder

---

4. FØRSTE RESPONS – HANDLINGSPLAN

De første minutter efter en cyberhændelse opdages er som de første minutter efter et trafikuheld - de beslutninger I træffer nu kan gøre forskellen mellem en mindre forsinkelse og en total katastrofe.

Statistikker viser at virksomheder som reagerer inden for de første 15 minutter kan reducere den samlede skade med op til 70% sammenlignet med dem der venter en time eller mere.

Hvorfor er tempo så kritisk? Cybertrusler udvikler sig eksponentielt. En enkelt inficeret computer kan sprede ransomware til hundredvis af andre maskiner på få minutter hvis netværksforbindelsen ikke brydes. Samtidig fortsætter hackere med at stjæle data eller installere flere skadelige programmer hver eneste minut de har adgang. Tænk på det som at slukke et hus der brænder - jo tidligere I kommer i gang med at slukke ilden, jo mindre skade bliver der.

FØRSTE 15 MINUTTER

De fleste cyberhændelser bliver først opdaget af en almindelig medarbejder der lægger mærke til at noget er anderledes. Det kan være en computer der opfører sig mærkeligt, en email der virker mistænkelig, eller systemer der pludselig er langsomme. Denne medarbejder bliver det første og ofte vigtigste led i forsvaret.

For den der opdager hændelsen:

1. STOP - Rør ikke ved mere end nødvendigt
2. Ring til IT-ansvarlig: [TELEFONNUMMER]
3. Dokumenter: Hvad så du? Hvornår? Hvilket system?
4. Isoler: Træk netværksstik hvis muligt (ikke sluk computer)

For IT-ansvarlig:

1. Bekræft hændelsen - Er det en reel trussel?
2. Klassificer - Niveau 1, 2 eller 3?
3. Aktiver team - Ring til relevante personer
4. Start logbog - Dokumenter alt fra nu af

FØRSTE TIME

Den første time er hvor I går fra initial reaktion til systematisk respons. Nu hvor I har fået overblik og aktiveret jeres team, skal I begynde den mere strukturerede proces med at begrænse skaden og forberede jer på genoprettelse. Brug denne tjekliste:

Teknisk respons:

- [ ] Isoler berørte systemer
- [ ] Vurder omfang af inficering
- [ ] Sikr bevismateriale
- [ ] Check backup-status
- [ ] Implementer midlertidige løsninger

Kommunikation:

- [ ] Informer ledelse
- [ ] Udarbejd intern meddelelse
- [ ] Vurder behov for ekstern kommunikation
- [ ] Kontakt forsikringsselskab (hvis relevant)

---

5. KRITISKE SYSTEMER OG BACKUP

At forstå hvilke systemer der er mest kritiske for jeres forretning, er som at kende forskel på hjerte, lunger og fingerneglen på en person - alle er en del af kroppen, men nogle er langt mere afgørende for overlevelse end andre. Mange virksomheder opdager for sent at de har brugt lige så mange ressourcer på at beskytte systemer der "ville være rart at have" som på systemer der "skal fungere for at vi kan overleve".

Hvorfor er system-prioritering afgørende? Under en cyberkrise har I begrænsede ressourcer og tid. Hvis I prøver at redde alt på én gang, risikerer I at miste alt. Ved at have en klar prioritering kan I fokusere jeres indsats på at få de mest kritiske systemer op at køre først, så virksomheden kan fortsætte med at fungere mens I arbejder på de mindre kritiske elementer. Dette kan være forskellen mellem at være lukket ned i timer versus dage.

Forretningsmæssig påvirkning af systemnedbrud: Dette kaldes også en BIA – Business Impact Amnalyse. Tænk på det sådan - hvis jeres e-mail-system er nede i fire timer, kan I stadig tage telefonen og betjene kunder. Men hvis jeres hovedsystem til at behandle ordrer er nede i fire timer, kan I måske miste en hel dags salg og frustrere kunder så meget at de skifter til konkurrenter. Det er derfor vi ikke kan behandle alle systemer ens.

System-prioritering (Tilpas til jeres virksomhed)

System	Prioritet	RTO	Backup-frekvens	Recovery-tid
Email-server	1	2 timer	Daglig	1 time
Økonomisystem	1	4 timer	Daglig	2 timer
Kundeportal	2	8 timer	Daglig	4 timer
Filserver	2	1 dag	Daglig	4 timer
Telefonanlæg	3	2 dage	Ugentlig	1 dag

Backup-Checklist

Backup er jeres livline når alt andet fejler, men kun hvis det fungerer når I har brug for det. Statistikker viser at op til 30% af virksomheder opdager at deres backup ikke virker først når de prøver at bruge det under en krise. Det er som at opdage at jeres brandslukker er tom når huset brænder.

- [ ] Daglig automatisk backup kører
- [ ] Ugentlig test af backup-restore
- [ ] Månedlig fuld restore-test
- [ ] Backup opbevares off-site (cloud eller fysisk)
- [ ] Backup-systemet er isoleret fra hovednetværk

6. KOMMUNIKATION UNDER KRISE

Kommunikation under en cyberkrise er som at være nyhedsoplæser under en naturkatastrofe - alle stirrer på jer for at få information, men I har kun begrænset viden og hver forkert eller forhastet udmelding kan skabe panik eller ødelægge tilliden for evigt. Samtidig er stilhed ofte værre end ufuldstændig information, fordi mennesker har en tendens til at forestille sig det værste når de ikke hører noget.

Psykologien bag krisekommunikation er en god indsigt at have. Under usikkerhed søger mennesker mod information og kontrol. Hvis I ikke giver dem troværdig information, vil de finde deres egne kilder - og disse kan være rygter, spekulationer eller direkte misinformation. Ved at være den første og mest pålidelige kilde til information om jeres egen krise, kan I kontrollere narrativet og bevare tilliden hos de mennesker der betyder mest for jeres virksomheds fremtid.

Forretningsmæssige konsekvenser af dårlig kommunikation. Studier viser at virksomheder kan miste op til 30% af deres kundebase efter en cyberhændelse - ikke nødvendigvis på grund af selve hændelsen, men på grund af hvordan de kommunikerede om den. Kunder kan tilgive tekniske problemer, men de tilgiver sjældent følelsen af at være blevet holdt i mørke eller løjet for.

Intern Kommunikation

Medarbejdere:

- Kanal: Email + intranet + opslag
- Timing: Inden for 1 time
- Ansvarlig: Kommunikationsansvarlig
- Template: "Vi oplever tekniske problemer og arbejder på en løsning. Brug IKKE [specificer systemer] indtil videre. Updates følger."

Ledelse:

- Kanal: Telefon + email
- Timing: Inden for 30 minutter
- Ansvarlig: IT-ansvarlig
- Indhold: Status, omfang, forventet løsning

Ekstern Kommunikation

Kunder:

- Hvornår: Kun hvis service påvirkes > 4 timer
- Ansvarlig: CEO/Kommunikationsansvarlig
- Kanal: Website, social medier, direkte kontakt
- Template: "Vi oplever midlertidige tekniske udfordringer. Vi arbejder intensivt på en løsning og beklager ulejligheden."

Leverandører:

- Hvornår: Hvis deres systemer påvirkes
- Ansvarlig: Indkøbschef/Driftschef

Myndigheder:

- Hvornår: Persondata berørt (72 timer til Datatilsyn)
- Ansvarlig: CEO + Juridisk rådgiver
- Krav: Følg nationalt regelsæt (GDPR)

---

7. ESCALATION OG EKSTERN HJÆLP

At vide hvornår man skal bede om hjælp er en af de sværeste beslutninger under en cyberkrise. Det er som at vide hvornår man skal ringe til ambulancen versus at køre selv til skadestuen - vent for længe og situationen kan blive katastrofal, men ring for tidligt og I kan spilde værdifulde ressourcer på et problem I kunne have løst selv. For SME-virksomheder, som typisk har begrænsede IT-ressourcer og budgetter, er denne balance særligt kritisk.

Mange ledere og IT-ansvarlige kæmper med at erkende at de har brug for ekstern hjælp. Der er en naturlig stolthed i at kunne løse problemer selv, og en bekymring for omkostningerne ved ekstern konsulenthjælp. Men under en cyberkrise kan denne tøven være forskellen mellem at redde virksomheden og at miste den helt.

Økonomien i ekstern hjælp under krise kan være en dyr fornøkelse. Cybersikkerhedskonsulenter er dyre - ofte 2.000-5.000 kr. i timen eller mere. Men sammenlign det med omkostningerne ved at være lukket ned i flere dage, miste kundedata, eller betale løsepenge til hackere.

En erfaren konsulent kan ofte løse på timer hvad det ville tage jeres interne team dage at finde ud af, og de har værktøjer og kontakter som I ikke har adgang til. Når virksomhedens overlevelse er på spil, er det ikke tiden til at spare på ekspertisen.

Hvornår skal vi eskalere?

- [ ] Hændelsen er ikke under kontrol efter 2 timer
- [ ] Kritiske systemer er berørt
- [ ] Persondata kan være kompromitteret
- [ ] Mistanke om organiseret kriminalitet
- [ ] Medieinteresse opstår

Ekstern hjælp – Kontaktliste

I cyberverdenen er der ikke et enkelt "112" nummer - I skal selv have identificeret og etableret relationer til de rigtige specialister før krisen rammer.

IT-Security leverandør:

- Firma: [NAVN]
- Kontakt: [NAVN + TLF]
- SLA: [RESPONSTID]
- Specialer: Incident response, forensics

Jurist/Advokat:

- Firma: [ADVOKATFIRMA]
- Kontakt: [NAVN + TLF]
- Specialer: IT-ret, GDPR

PR/Krisekommunikation:

- Firma: [NAVN]
- Kontakt: [NAVN + TLF]
- Tilgængelighed: 24/7

Forsikring:

- Selskab: [NAVN]
- Policenummer: [NUMMER]
- Kontakt: [NAVN + TLF]

---

8. RECOVERY OG GENOPRETTELSE

Recovery-fasen er hvor I går fra "vi overlever krisen" til "vi er stærkere end før krisen". Det er her mange virksomheder laver deres største fejl - de bliver så lettede over at have stoppet det akutte problem at de skynder sig tilbage til "normal" drift uden at sikre sig at truslen virkelig er elimineret og at deres systemer er mere sikre end før angrebet.

Forskellen mellem "virker" og "er sikkert": En computer der kan starte op og køre programmer "virker", men det betyder ikke at al skadelig software er fjernet eller at hackere ikke stadig har adgang. En email-server der kan sende og modtage mails "virker", men alle passwords kan stadig være kompromitterede. Recovery handler ikke kun om at få tingene til at fungere igen - det handler om at gendanne sikkerhed og tillid.

Statistikker viser at virksomheder der skynder sig gennem recovery-fasen har 3x højere risiko for at blive ramt af samme type angreb igen inden for 6 måneder. Dette skyldes at de ikke har elimineret alle spor af den oprindelige trussel eller lukket de sikkerhedshuller der gjorde det første angreb muligt. At skulle gennem samme krise to gange er ikke kun dyrt - det kan være dødsstødet for kundetillid og virksomhedens omdømme.

Efter timer eller dage med intens krise er dit team mentalt udmattet og vil naturligt presse på for at "komme videre". Men det er netop når man er træt at man laver de

kritiske fejl. Systematisk recovery sikrer at ingen vigtige skridt springes over, selv når alle bare vil have normalitet tilbage.

Recovery-faser

At opdele recovery i tydelige faser hjælper med at sikre at intet vigtigt springes over, og at I ikke erklærer sejr for tidligt. Hver fase har specifikke mål og succeskriterier der skal være opfyldt før I kan gå videre til næste fase.

Fase 1: Stabilisering

- [ ] Truslen er elimineret
- [ ] Systemer er sikret
- [ ] Midlertidige løsninger fungerer
- [ ] Kommunikation er håndteret

Fase 2: Genoprettelse

- [ ] Systemer gendannes fra backup
- [ ] Funktionalitet testes
- [ ] Brugere får adgang gradvist
- [ ] Overvågning af stabilitet

Fase 3: Normalisering

- [ ] Alle systemer fungerer normalt
- [ ] Backup-rutiner er opdateret
- [ ] Sikkerhedsforanstaltninger justeret
- [ ] Medarbejdere informeret om ændringer

Recovery-checklist

- [ ] Verificer at truslen er fjernet
- [ ] Test alle kritiske funktioner
- [ ] Skift passwords på alle systemer
- [ ] Opdater antivirusprogrammer
- [ ] Gennemfør sikkerhedsaudit

En post-incident sikkerhedsaudit skal identificere alle de måder angrebet kunne have været forhindret og sikre at lignende angreb ikke kan lykkes i fremtiden. Dette inkluderer tekniske sårbarheder, procedurefejl, og menneskelige faktorer. Ofte er det værdifuldt at få en ekstern part til at udføre denne audit for at få et objektivt perspektiv. Husk også at debreefe medarbejdere og anden personale.

---

9. EFTER HÆNDELSEN – LÆRING

Fasen efter en cyberhændelse er hvor I har mulighed for at transformere en traumatisk oplevelse til en værdifuld læring der gør jeres virksomhed stærkere. Mange

virksomheder springer denne fase over fordi alle bare vil "komme videre" og glemme den ubehagelige oplevelse. Men det er en enorm spildt mulighed - kriser er de bedste læringsøjeblikke fordi alle detaljer er friske i hukommelsen og motivationen for forbedring er høj.

Under normal drift er det svært at få folk til at fokusere på hypotetiske trusler eller abstrakte sikkerhedsrisici. Men efter en reel krise forstår alle præcis hvorfor cybersikkerhed er vigtig og er motiverede for at forhindre gentagelse. Dette er jeres mulighed for at implementere forbedringer der normalt ville møde modstand eller blive deprioriteret.

Virksomheder der bruger post-incident læring godt, ender ofte med en stærkere sikkerhedskultur end de havde før krisen. Medarbejdere der har oplevet konsekvenserne af cybertrusler bliver naturlige ambassadører for sikkerhedsforanstaltninger og er mere tilbøjelige til at følge sikkerhedsprocedurer og rapportere mistænkelige aktiviteter.

Selv en dyr cyberkrise kan blive en god investering hvis den forhindrer en endnu værre krise i fremtiden. Virksomheder der lære systematisk fra hændelser reducerer deres risiko for gentagelse med op til 85% og har typisk betydeligt lavere cyberforsikringspræmier fordi forsikringsselskaber anerkender deres forbedrede

Post-Incident Review (Inden for 1 uge)

Deltagere: Alle fra respons-teamet + CEO
Varighed: 2-3 timer
Ansvarlig: IT-ansvarlig

Agenda:

1. Hvad skete der? - Kronologisk gennemgang
2. Hvad gik godt? - Positive observationer
3. Hvad kunne være bedre? - Forbedringspunkter
4. Konkrete handlinger - Hvem gør hvad hvornår?

Dokumentation

- [ ] Komplet incident-rapport
- [ ] Opdateret risiko-vurdering
- [ ] Revideret beredskabsplan
- [ ] Medarbejder-briefing om lessons learned

Opfølgning

- [ ] Implementer forbedringspunkter
- [ ] Opdater træning/øvelser
- [ ] Revidér forsikringsdækning
- [ ] Planlæg næste beredskabsøvelse

10. VEDLIGEHOLDELSE AF PLANEN

En cyber beredskabsplan er som et træningsprogram for atleter - den er kun så god som den seneste gang den blev testet og opdateret. I cybersikkerhedsverdenen ændrer trusselsbilledet sig konstant, nye sårbarheder opdages, teknologier udvikler sig, og jeres egen virksomhed vokser og ændrer sig. En plan der var perfekt for seks måneder siden kan være helt utilstrækkelig i dag.

Cyberkriminelle innoverer konstant og udvikler nye angrebsmetoder for at omgå eksisterende forsvar. Samtidig ændrer jeres teknologiske infrastruktur sig - nye systemer tilføjes, gamle fjernes, medarbejdere skifter, og forretningsprocesser udvikler sig. En static plan kan ikke følge med denne hastighed af forandring.

En forældet beredskabsplan kan være værre end slet ingen plan, fordi den giver en falsk sikkerhedsfølelse. Teams kan spilde kritisk tid på at følge procedurer der ikke virker, kontakte personer der ikke længere er i virksomheden, eller prøve at gendanne systemer der er ændret siden planen blev skrevet. Under en krise er der ikke tid til at debugge en forældet plan.

Virksomheder der systematisk vedligeholder deres beredskabsplaner har ikke kun bedre respons-kapacitet - de har også bedre forståelse af deres egen IT-infrastruktur og risici. Denne dybere indsigt giver dem mulighed for at træffe bedre strategiske beslutninger om teknologi-investeringer og sikkerhedsforanstaltninger.

Månedlige opgaver

Månedlige opgaver fokuserer på at holde de mest kritiske og foranderlige elementer af planen aktuelle. Disse er opgaver der ikke kan vente til kvartals- eller årsgennemgang fordi de kan blive forældede meget hurtigt.

- [ ] Verificer kontaktoplysninger
- [ ] Test backup-systemer
- [ ] Gennemgå trussel-landskab
- [ ] Opdater incident-team

Kvartalsvise opgaver

Kvartalsvise opgaver fokuserer på mere omfattende tests og evalueringer der kræver betydelige ressourcer eller koordination mellem flere personer.

- [ ] Gennemfør tabletop-øvelse
- [ ] Revidér system-prioritering
- [ ] Opdater kommunikations-templates
- [ ] Evaluér ekstern leverandører

Årlige opgaver

Årlige opgaver er de mest omfattende og strategiske elementer af plan-vedligeholdelse. De kræver ofte betydelige ressourcer og involvering af senior ledelse.

- [ ] Fuld gennemgang af plan
- [ ] Stor beredskabsøvelse
- [ ] Forsikringsgennemgang
- [ ] Strategisk risiko-vurdering

---

11. HURTIG-REFERENCE KORT

PRINT UD OG HÆNG OP SYNLIGT!

🚨 CYBER-HÆNDELSE OPDAGET? 🚨

1. RING TIL IT-ANSVARLIG: [TELEFON]
2. DOKUMENTER: Hvad/Hvornår/Hvor
3. ISOLER: Træk netværksstik (sluk IKKE)
4. VENT på instruktioner

NIVEAU 3 HÆNDELSE?

→ Ring OGSÅ til CEO: [TELEFON]

→ Ring til ekstern IT: [TELEFON]

HUSK: PANIK HJÆLPER IKKE!

DOKUMENTER ALT - RING TIL HJÆLP

HUSK: Denne plan er kun så god som den træning og de øvelser I laver!

Planlæg jeres første tabletop-øvelse inden for 30 dage efter implementering.