Cyberberedskabsplan

Værktøjet er tilvejebragt i projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), der er støttet med midler fra Industriens Fond. Dato for publicering: 09.01.2026

Cyberberedskabsplan

- En cyberberedskabsplan er et dokument, der beskriver, hvordan en virksomhed **forebygger**, **opdager**, **håndterer** og **genopretter** sig efter cyberhændelser som f.eks. hackerangreb, ransomware, datalæk eller systemnedbrud.
- Planen fungerer som en operativ drejebog, der skal sikre hurtig, koordineret og korrekt handling, når noget går galt.

- **Formål og omfang**
  - Formål:
    - Forebygge og håndtere cyberangreb.
    - Minimere konsekvenser for produktion, data og kunder.
    - Sikre hurtig reaktion, kommunikation og genopretning.
  - Omfang:
    - Alle IT-systemer, produktionsstyringssystemer, ERP, CRM, netværk, servere, cloud-tjenester.
    - Alle medarbejdere, kontraktpartnere og eksterne leverandører med adgang til systemer.

Roller og ansvar (eksempler)

Rolle	Ansvar	Kontaktinformation	Backup
Krisestabsleder	Overordnet beslutningstagning under cyberkrise	Navn Telefon E-mail	CEO
IT-chef	Teknisk håndtering af angreb, isolation og genopretning	Navn Telefon E-mail	IT-support
Kommunikationsansvarlig	Intern og ekstern kommunikation	Navn Telefon E-mail	Kommunikations-medarbejder/CEO
HR-chef	Håndtering af personale og sikkerhedsprocedurer	Navn Telefon E-mail	HR-medarbejder
Compliance / GDPR ansvarlig	Rapportering til myndigheder og kunder	Navn Telefon E-mail	Juridisk rådgiver (intern/ekstern)

Handleplan (tjekliste) ved mistanke om cyberangreb

- Isolér berørte systemer (frakobl netværk).
- Informér IT-ansvarlig og krisestab.
- Stop spredning (luk konti, skift adgangskoder).
- Vurder påvirkning (IT, produktion, data).
- Gendan systemer fra backup.
- Kommunikér internt/eksternt efter plan.
- Dokumentér hændelsen.

Incident Response Plan – hvis uheldet er ude

Hændelse	Klassificering	Hvad gør vi? (reaktiv handlig)	Ansvarlig (eksempler)
Phishing-forsøg/mistænkelig e-mail	Lav	Advar modtager og andre medarbejdere Rapporter hændelsen til IT Slet e-mail og links	IT-chef
Malware/virus på en arbejdsstation	Medium	Isoler den inficerede maskine fra netværk Kør antivirus/malware-scanning Identificer og fjern skadelige filer Evaluer om andre systemer er påvirket	IT-chef
Ransomware-angreb på produktionssystemer	Høj	Isoler alle berørte systemer straks Aktivér incident response plan Informer krisestab og ledelse Gendan systemer fra sikre backups Underret myndigheder, hvis relevant	IT-chef/krisestabsleder
Databrud/kompromittering af kundedata	Høj	Identificer hvilke data er påvirket Informer ledelse og databeskyttelsesansvarlig (GDPR) Underret berørte kunder og myndigheder inden for lovpligtige tidsfrister Sæt sikkerhedsforanstaltninger op for at forhindre yderligere adgang	IT-chef/krisestabsleder

Kommunikationsplan (eksempler)

Målgruppe	Kanal	Ansvarlig	Budskab	Tidspunkt
Medarbejdere	E-mail, telefon, intranet	HR / Kommunikationsansvarlig	Instrukser, opdateringer	Umiddelbart efter hændelse
Kunder	E-mail, telefon, website	Kommunikationsansvarlig	Informer om forsinkelser, datahændelser	Senest 4 timer efter hændelse
Leverandører	E-mail, telefon	Indkøb	Status på leverancer / systemadgang	Umiddelbart efter hændelse
Myndigheder	E-mail, telefon	Krisestabsleder / Compliance / CEO	Lovpligtig rapportering	Så snart det er nødvendigt

Forebyggende (proaktive) tiltag (eksempler)

1. Antivirus og firewall på alle enheder.
2. Netværksovervågning.
3. MFA (Multi-Factor Authentication) (flerfaktorautentifikation) på kritiske systemer. Man skal bekræfte ens identitet med to eller flere forskellige typer beviser (faktorer) for at få adgang til data/systemer.
4. Patch- og opdateringspolitik (en patch er en opdatering til et software).
5. Sikkerhedstest / penetrationstest.
6. Backup af kritiske systemer og data: Daglig, testet, offline + cloud.
7. Awareness-træning for medarbejdere i phishing og social engineering.

Reaktive strategier

- Incident response plan med roller og trin-for-trin handling.
- Isolation af inficerede systemer.
- Gendannelse fra backup.
- Kommunikation til medarbejdere, kunder og myndigheder.
- Evaluering og opdatering af sikkerhedspolitikker.

Træning og test (eksempler)

- Simulering af cyberangreb (phishing, malware, ransomware) 1-2 gange årligt.
- Træning af krisestab og IT-personale.
- Dokumentation af øvelser og evaluering af forbedringspunkter.

Vedligeholdelse (eksempler)

- Opdater kontaktoplysninger og roller hver 6. måned.
- Revider klassificering af risici og strategier årligt.
- Evaluer og opdater planen efter hver øvelse eller reel hændelse.
- Sørg for at alle medarbejdere har adgang til nyeste version.