# Incidenthanteringsplan

Organisation:

Version:

Datum:

Godkänd av:

CYLOQ

# 1

# Syfte och scope

Denna plan beskriver hur *organisationens namn:* identifierar, hanterar och återhämtar sig från cybersäkerhetsincidenter. Syftet är att minimera skada, uppfylla rapporteringsskyldigheter och säkerställa att organisationen kan återgå till normal drift så snabbt som möjligt.

Vad räknas som en incident?

En incident är en händelse som påverkar eller riskerar att påverka konfidentialitet, integritet eller tillgänglighet hos organisationens system eller data.

## Allvarlighetsnivåer:

| Nivå | Beskrivning | Exempel |
|---|---|---|
| Kritisk | Pågående intrång, data exfiltreras, affärskritiska system nere | Ransomware, aktivt intrång |
| Hög | Misstänkt kompromittering, känslig data exponerad | Kontokompromettering, dataintrång |
| Medel | Begränsad påverkan, inga bevis på exfiltrering | Skadlig kod isolerad, phishing-försök |
| Låg | Säkerhetsvarning utan bekräftad påverkan | Misslyckade inloggningsförsök |

# 2 Roller och kontaktuppgifter

## Incidentteam

| Roll | Namn | Telefon | E-post | Backup |
|---|---|---|---|---|
| Incidentledare | | | | |
| Tekniskt ansvarig | | | | |
| CISO / Säkerhetschef | | | | |
| Juridisk rådgivare | | | | |
| Kommunikations-ansvarig | | | | |
| VD / Ledning | | | | |

## Externa kontakter

| Organisation | Kontakt | Telefon | När kontaktas de |
|---|---|---|---|
| Extern säkerhetsleverantör | | | Vid alla kritiska och höga incidenter |
| Cyloq (incidentstöd) | | 010-333 10 33 | Vid behov av extern forensik eller stöd |
| Försäkringsbolag | | | Inom 24 timmar vid incident |
| MSB | | | Inom 24 timmar (NIS2) |
| IMY | | | Inom 72 timmar (GDPR) |
| Polisen / NOA | | | Vid utpressning eller betydande skada |

# 3

# Kommunikationsplan

## Intern kommunikation

- Incidentledaren ansvarar för dagliga lägesuppdateringar till ledningen så länge incidenten pågår.
- Övriga medarbetare informeras när ett korrekt och fullständigt budskap kan ges.
- Kommunikationskanal under incident: _____

## Extern kommunikation

- Vem har mandat att uttala sig externt: _____
- Godkännandeprocess för externa uttalanden: _____
- Kunder informeras om deras data berörs, efter att scope är bekräftat.
- Medieförfrågningar hanteras av: _____

## Kommunikationsmallar

Förbered färdiga kommunikationsmallar för de scenarier som är mest relevanta för er verksamhet. Exempel på scenarier: dataintrång, ransomware, driftstörning. En mall bör innehålla: vem kommunikationen riktar sig till, vad som hänt (i generella termer), vad ni gör åt det och vad mottagaren behöver göra.

# 4

# Tekniska runbooks

## 4.1 Ransomware

1. Isolera drabbade system – koppla bort nätverket men stäng inte av maskinerna.
2. Identifiera vilka system som är krypterade och hur långt intrånget nått.
3. Säkra loggar från brandvägg, AD och endpoint omedelbart.
4. Kontakta extern säkerhetsexpert.
5. Kontakta försäkringsbolag inom 24 timmar.
6. Rapportera till MSB inom 24 timmar (NIS2) och IMY inom 72 timmar om persondata berörs.
7. Påbörja återställning från verifierade backuper – återanslut inte system förrän de är granskade.
8. Betala inte lösensumma utan juridisk rådgivning.

## 4.2 Dataintrång / obehörig åtkomst

1. Identifiera vilket konto eller system som är kompromitterat.
2. Spärra berörda konton och återkalla åtkomst.
3. Säkra loggar för forensisk analys.
4. Bedöm vilken data som kan ha exponerats.
5. Kontakta extern expert vid behov.
6. Rapportera till IMY inom 72 timmar om persondata berörs.
7. Informera berörda kunder när scope är bekräftat.

## 4.3 DDoS

1. Kontakta internetleverantör och aktivera eventuellt DDoS-skydd.
2. Dokumentera angreppsmönster och tidpunkt.
3. Bedöm om angreppet är ett rökridå för ett annat intrång – kontrollera övriga system parallellt.
4. Kommunicera driftstörning internt och externt vid behov.

## 4.4 Kontokompromettering

1. Spärra det kompromitterade kontot omedelbart.
2. Återkalla aktiva sessioner och tokens.
3. Granska loggar för att bedöma vad kontot haft åtkomst till.
4. Återställ lösenord och aktivera MFA om det saknades.
5. Bedöm om angriparen rört sig till andra system eller konton.

# 5

# Rapporteringskrav och tidsfrister

| Myndighet / Part | Frist | Villkor | Ansvarig |
|---|---|---|---|
| MSB (NIS2 – initial) | 24 timmar | Väsentliga/viktiga entiteter | |
| MSB (NIS2 – fullständig) | 72 timmar | Väsentliga/viktiga entiteter | |
| IMY (GDPR) | 72 timmar | Om persondata berörs | |
| Försäkringsbolag | 24 timmar | Kontrollera villkor | |
| Polisen / NOA | Snarast | Vid utpressning eller betydande skada | |

# 6

# Återställningsrutiner

## Prioriteringsordning för återställning

(Lista era affärskritiska system i prioriteringsordning)

| Prioritet | System | Ansvarig | Beroenden |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

## Återställningsprinciper

- Återställning sker alltid från verifierade, rena backuper.
- System återansluts inte till nätverket förrän de är forensiskt granskade och härdade.
- Godkännande för återstart ges av: _____
- Backuper finns på följande platser: _____
- Senaste verifierade backup-test: _____

# 7

# Lessons learned-process

## Efter varje incident ska följande genomföras inom 2 veckor:

1. **Genomgång med incidentteamet** – vad hände, i vilken ordning och varför?
2. **Identifiering av rotorsaken** – hur tog angriparen sig in och vad möjliggjorde det?
3. **Dokumentation av lärdomar** – vad fungerade, vad fungerade inte?
4. **Uppdatering av planen** – anpassa rutiner, kontaktuppgifter och runbooks baserat på incidenten.
5. **Åtgärdsplan** – konkreta förbättringsåtgärder med ansvarig och deadline.

## Mall för lessons learned-rapport:

- Datum för incident: _____
- Incidenttyp och allvarlighetsnivå: _____
- Tidslinje: _____
- Rotorsak: _____
- Åtgärder vidtagna: _____
- Förbättringsåtgärder: _____
- Ansvarig för uppföljning: _____

8

# Underhåll och versionshantering

| Aktivitet | Frekvens | Ansvarig |
|---|---|---|
| Genomgång och uppdatering av hela planen | Minst en gång per år | |
| Verifiering av kontaktuppgifter | Kvartalsvis | |
| Tabletop-övning | Minst en gång per år | |
| Uppdatering efter incident | Efter varje incident | |
| Godkännande av ledningen | Minst en gång per år | |

Mallen är framtagen av **Cyloq** och anpassad för svenska organisationer med NIS2- och GDPR-krav. För hjälp med implementering eller säkerhetstester – kontakta oss på **010-333 10 33** eller **cyloq.se**.