Rutin: Kritiska incidenter, Critical Incident

Version av rutin – 1.0
Datum – 2018-11-01
Författare – Daniel Öfverstedt, PrimeQ Outsourcing AB
Ansvarig – CEO PrimeQ Outsourcing AB
Ändringshantering:
Ver 1.0: Skapande av rutin

Innehållsförteckning

Introduktion

Följande rutin etablerar en standard och process för hanteringen av kritiska incidenter i PrimeQs (eller kund i PrimeQs) IT miljö. Rutinen skall ses som en vägledning hur man bör hantera incidenter av allvarlig art.

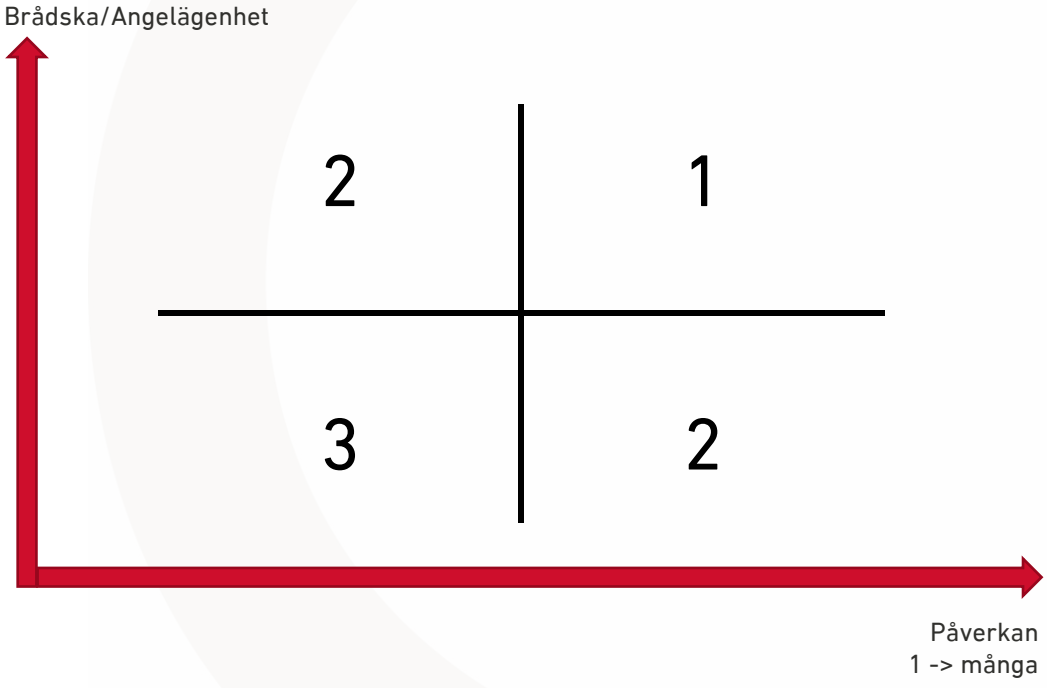
OBS! Aktiveras rutinen skall den följas till sin helhet, d.v.s. det finns inga grader av stor eller liten kritisk incident, alla punkter skall följas.

Omfattning

Rutinen/förfarandet omfattar kritiska incidenter där problemen medför total stopp i ett system/applikation eller medför kraftigt begränsade möjligheter att använda en applikation, system eller utrustning vilka är avgörande för koncernens (eller driftkund till koncernens) verksamhet.

Prioritering av incident

En incident bör prioriteras enligt nedanstående modell där prioritet 1 bör anses som kritiskt och då skall rutinen följas. Även en prio-2 incident kan i vissa fall föranleda att rutinen aktiveras.



Roller

Tekniskpersonal – IT personal vilka arbetar med att diagnostisera och finna en lösning till problemet – vanligen från interna organisationen tillsammans med leverantör/er
Incident Manager – är en erfaren person ur Servicedesk eller driftorganisation hos PrimeQ alt. leverantör.
Denna roll skall alltid vara bemannad av PrimeQ under servicetid.
Critical Incident Manager – erfaren ledande person, vilken kallas in enligt ordning nedan vid kritiska incidenter:

Eskaleringsordning CIM

Följande ordning nedan beskrivs hur incidenten skall eskaleras för att bemanna CIM rollen, alternativt när behov finns att eskalera internt för att få rätt beslut fattade.

En incident kan klassificeras som kritisk av:

- Teknisk personal hos PrimeQ
- Teknisk behörig personal hos kund
- Incident manager hos kund eller PrimeQ
- VD/CIO hos kund

CIM tillsätts enligt följande ordning:

- CIM
- Driftchef
- CIO

För aktuell information om vilken person som har rollen/rollerna se:
https://primeq.se/xxxxxxxxxx

Ansvarsbeskrivning CIM

I rollen som Critical Incident Manager ingår att säkerställa att:

- Korrekta insatser tas i rätt tid.
- Definierade/dokumenterade rutiner följs.
- Rätt resurser arbetar med att lösa problemet.
- Rätt information kan besvaras enligt strukturen;
  -Vad har hänt?
  -Varför hände det?
  -Hur stor är omfattningen samt konsekvenser av det som har hänt

-Vad har vi gjort och vad gör vi för att lösa problemet
-Om problemet inte är löst, när tror vi att det är löst
-Hur ser vi till att detta inte händer igen

- Om nödvändigt använda positionens auktoritet för att säkerställa att (rätt) fokus koncentreras till att lösa problemet.

Checklista Critical Incident Manager (CIM)

När en kritisk incident inträffar är CIM ansvarig för följande:

☐ **Dokumentera incidenten**
- Löpande under incidenten föra noteringar med klockslag om beslut, möten, tester etc. för incidentrapporten

☐ **Prioritera händelsen tillsammans med verksamheten enligt modellen Brådska/Påverkan**
- Hur Brådskande/Angeläget är det?
- Hur många är påverkade?

☐ **Avstämning med leverantör**
Säkerställa att de inledande aktiviteterna är genomförda, dvs:
- Ärendet är registrerat som kritisk incident hos PrimeQ alt. Leverantören.
- Personal hos PrimeQ eller motsvarande finns allokerad att arbeta med incidenten.

☐ **Kommunikation**
Vid behov skall en telefonkonferens initieras via SMS anrop till angivna kontaktpersoner där berörda eller samtliga skall ringa in för att ta del av händelseförloppet samt delges uppdrag för att lösa incidenten. Detta effektiviserar arbetet då vi snabbt kan nå varandra, har samma statusinformation, minskar risken för missförstånd och/eller att flera felsöker på samma sak.

Kontaktpersoner PrimeQ: https://primeq.se/xxxxxx
Kontaktpersoner kund: ?

- **Kommunikation med berörda ledningspersoner**
  - Kund har ansvar för att informera internt inom sin egen organisation.
  - PrimeQ ansvarar för att informera inom sin egen organisation

☐ **Kommunikationskanaler:**

- Första information kring att CIM är initierad skall ske per SMS. Utskick görs via: https://www.xxxxxxxx.se (användarnamn och lösenord i lösenordshanteraren)
  - Det finns en färdiga distributionslistor under menyn ”Listor”
  - Vid behov av telefonkonferens ska följande telefonnummer samt kod användas:
    Nummer: 08-xxxxxxxx - Kod: xxxxxxxx
  - Efterföljande information skickas löpande per mail.
  - Eftersträva att alltid kunna besvara:
    - Vad har hänt?
    - Varför hände det?
    - Hur stor är omfattningen samt konsekvenser av det som har hänt?
    - Vad har vi gjort och vad gör vi för att lösa problemet?
    - Vad får ev. workarounds för konsekvenser?
    - Om problemet inte är löst, när tror vi att det är löst?
    - Hur ser vi till att detta inte händer igen?

☐ **Säkerställa att rätt resurser är allokerade.**
Verifiera att rätt resurser är allokerade för att lösa problemet.
Exempel: har man rätt team som arbetar med problemet, är personerna tillräckligt erfarna för att lösa problem av denna karaktär?

Överbrygga alla hinder, vilka försvårar för de allokerade resurserna att uteslutande kunna koncentrera sig på problemet.
Exempel: är det för många personer som kräver information om status, tillgång till kompetens grupper etc.

Oavsett vad de allokerade resurserna behöver är det Critical Incidents Managerns ansvar att se till att de får det som efterfrågas.

☐ **Plan A och Plan B**
Kan vi arbeta på parallella spår för att vinna tid?

Exempel: Om servern inte startar efter diskbytet, har backupåterläsning startats till isolerad miljö? Behöver vi köpa in en ny server?

☐ **Planering av långsiktiga aktiviteter.**
Ordna möte med berörda personer

Exempel: när måste nästa skift sättas in, behövs reservutrustning osv...

☐ **Leverantörssupport.**
Förvissa sig om att man har betänkt/övervägt om externa leverantörer skall kallas in. Som regel skall alltid leverantörer kallas in när det gäller kritiska incidenter

☐ **Pågående problemlösning.**

- Om problemet ej kan lösas inom 1 timme, skall CIM kalla till ett kritiskt incident möte/telefonkonferens för att:
    - få komplett briefing från personalen som arbetar med störningen
    - genomföra analyser av effekter och pågående risker
    - granska tillvägagångssättet för att lösa ärendet
    - bestämma alternativa vägar (om möjliga)
    - utveckla beredskapsplaner
    - säkra att rätt resurser är allokerade (även externa leverantörer)
    - informera operativa chefer, verksamhetschefer och marknadschefer

Beroende på vilken typ av problem man hanterar skall CIM bestämma tätheten mellan team möten och säkra att dessa hålls. Rekommendationen är att möten minst hålls varannan timme.

Avslutad incident

- Genomför debriefing med medverkande personal i nära anslutning till att normal funktionalitet är återställd. Berör problemets uppkomst, agerandet och lösningen. Vilka lärdomar har man gjort, vilka insatser kan göras för att hindra eller lindra liknande händelser?
- CIM skall sammanställa och avleverera incidentrapporten, enligt framtagen mall. Rekommendation att ej skriva rapport omedelbart efter utan ge viss tid till reflektion och komplett faktainsamling. Rapporten skall vara klar inom 3 dagar efter avslutad incident.

Ansvarig för rutinen

CEO PrimeQ Oursourcing AB