Engineer

Hendelseshåndtering

⏏ samordning av tiltak og avgjørelser under en hendelse

Hva det er

Hendelseshåndtering er arbeidet med å samordne tiltak når en tjeneste svikter eller et system står overfor en alvorlig trussel. Hendelsen er det som utløser innsatsen. Håndteringen omfatter å oppdage og erklære hendelsen, fordele arbeidet, gjenopprette en brukbar tjeneste og overlate gjenværende oppgaver til navngitte personer. Utvikling, drift og brukerstøtte kan bidra. Ved noen hendelser trengs også personer som kan ta juridiske beslutninger eller avgjøre hvordan berørte skal beskyttes.

NISTs anbefalinger for sikkerhetshendelser beskriver oppdagelse, håndtering og gjenoppretting, med forberedelse og løpende forbedring som støtte. Publikasjonen gjelder cybersikkerhet. Tydelig ansvarsfordeling har også verdi når en ny versjon gir driftsstans. Ved mulig utlevering av data kan det være nødvendig å bevare bevis og ta vare på brukerne selv om tjenesten fremdeles svarer. Ved et vanlig driftsavbrudd kan første oppgave være å finne en trygg vei tilbake for trafikken.

Googles beskrivelse av hendelsesledelse skiller mellom en innsatsleder, en ansvarlig for tiltak i driften og en ansvarlig for kommunikasjon. Én person kan fylle flere roller i starten. Når flere kommer til, gir det mening å skrive ned hvem som har hvilket ansvar. Folk slipper da å gjette hvem som leder endringene, samler opplysninger eller sender en oppdatering. Rollene kan fordeles etter situasjonen og størrelsen på teamet.

Bruk begrepet i en beslutning

Bruk «Hva er hendelseshåndtering?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Overvåking og varsler som sier fra mens en feil fortsatt er liten, og tallene som viser hvor ofte den holder seg liten.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Bygde selskapets første observerbarhetsdashbord — selskapets første innsyn i egne systemer

Bygde selskapets første observerbarhetsdashbord Ta kontakt →

Hvorfor det er viktig

Tidlig i en hendelse kommer opplysningene i forskjellig tempo. En måling kan vise at betalinger svikter, mens det tar tid å finne ut hvilke kunder eller betalingsmåter som rammes. Brukerstøtten kan få et tydelig mønster før driften gjør det. En felles tidslinje samler observasjoner, kilder og usikkerhet. Da kan andre undersøke uten å anta at den første forklaringen er riktig.

Håndteringen gir også kontroll med endringer som må gjøres under press. Å rulle tilbake og endre en innstilling kan begge være fornuftig, men kombinasjonen kan få en uønsket virkning. Den som samordner, trenger å vite hva hver deltaker vil gjøre, når resultatet blir synlig og hvordan endringen eventuelt reverseres. Fagfolk kan foreslå løsninger, og teamet vet hvem som kan beslutte tiltak som berører andre.

Gjenoppretting og årsaksarbeid har ulik tidsramme. Å rute trafikken bort fra en del av systemet som svikter, kan gi brukerne tjenesten tilbake før årsaken er fastslått. Teamet kan markere gjenoppretting når konkrete kriterier er oppfylt, for eksempel at nye bestillinger går gjennom og at avvik i tidligere bestillinger følges opp. En senere gjennomgang ser på hvorfor hendelsen oppsto og hvordan håndteringen virket. Den trenger dokumentasjon om målinger, valg og usikkerhet.

Slik ser det ut i praksis

Tenk deg en billettjeneste som noen ganger trekker betalingen uten å utstede billetten. Brukerstøtten ser de første meldingene, og utvikling bekrefter at noen forespørsler feiler. Den som tar første vakt, erklærer en hendelse og skriver ned tidspunktet da symptomene ble oppdaget. Teamet blir enig om en kort beskrivelse av virkningen og navngir den som samordner endringene. Brukerstøtten får en kontaktperson og et tidspunkt for neste oppdatering.

Driften ser gjennom et utvalg bestillinger og finner en nylig endring som kan forklare tidspunktet. Innsatslederen ber gruppen sjekke at tidligere betalinger fortsatt blir synlige hvis programvaren rulles tilbake. En person gjennomfører

endringen, og en annen følger betalinger og billettutstedelser. Brukerstøtten bevarer bestillingsnumrene som må følges opp. En beskjed til kundene forklarer hva de kan gjøre med en uavklart bestilling og kan endres når teamet vet mer.

For å bekrefte resultatet sjekker teamet hele transaksjoner, særlig at betalingen og billetten stemmer overens. Det følger også arbeidet med å rydde opp i saker som ble stående. Når tjenesten er brukbar, registreres tidspunktet og hvem som tar de uavklarte bestillingene. Teamet kan avslutte innsatsen når ordinær drift kan overta den gjenværende risikoen. Undersøkelsen av årsaken kan fortsette med en avtalt ansvarlig og frist.

Engineers sak om voksende minnebruk i en macOS-app viser separate målinger og arbeidet med å begrense mengden hendelsesdata som ble beholdt. Den viser hvorfor det er viktig å bevare hva hvert resultat faktisk dekker. Billettjenesten er et tenkt eksempel på koordinering og oppfølging.

Ved vaktskiftet går avtroppende og påtroppende ansvarlig gjennom de siste beslutningene sammen. De merker hva som er bekreftet, hvilke tiltak som fortsatt kjører og når det kommer en ny beskjed. Dermed kan den som tar over, fortsette uten å lete gjennom meldinger mens noen venter på en beslutning.

Hvor det går galt

Teamet venter til det er helt sikkert. En sannsynlig virkning kan undersøkes med en navngitt ansvarlig og en avtalt oppdatering. Bestem hva som utløser en samordnet innsats. Den kan avsluttes hvis det viser seg at virkningen var mindre alvorlig.

Flere endrer systemet samtidig. Bruk en kort felles logg for de foreslåtte tiltakene og hvem som utfører dem. Se hva ett tiltak gjorde før du legger til et nytt hvis det er mulig. Si hvilke oppgaver som kan foregå uavhengig.

Kundene får høre gjetninger. Beskriv virkningen de kan oppleve, hva de trygt kan gjøre og når de får nytt. Si hva som fortsatt er usikkert. Vent med forklaringen av årsaken til den kan underbygges.

Alt annet forsvinner når driften er tilbake. Gi rydding, kundekontakt og midlertidige tiltak en ansvarlig. Før oppgavene over til stedet der teamet følger arbeidet til vanlig.

Les mer

- NIST SP 800-61 Rev. 3 — sikkerhetshendelser, forberedelse og forbedring.
- Google om ledelse av hendelser — roller, kommunikasjon og felles hendelseslogg.
- Hendelseshåndtering i Googles SRE-arbeidsbok — eksempler og erfaringer fra faktisk praksis.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er hendelseshåndtering?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

welcome@engineer.company +45 50 10 61 84 København, Danmark

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/incident-response/