Engineer

Driftshendelse

en hendelse som truer et systems data eller tjeneste

Hva det er

En driftshendelse, på engelsk incident, er et problem i et system i drift som har blitt alvorlig nok til at folk legger bort det planlagte arbeidet og tar seg av det med en gang: en tjeneste som har sluttet å svare, poster som er endret, en maskin som har gått tom for minne, en konto som noen andre bruker. Sikkerhetsfolk sier sikkerhetshendelse, driftsfolk sier driftshendelse eller rett og slett nedetid, og de fleste organisasjoner sorterer hendelsene sine i alvorlighetsgrader.

Veiledningen fra NIST om håndtering av hendelser trekker grensen i tre trinn, og de holder godt også utenfor sikkerhetsfaget. En hendelse, event, er alt som kan observeres og som involverer IT-ressurser: et innloggingsforsøk, en programvareoppdatering, en app som svarer på en forespørsel. En uønsket hendelse er en som får negative følger, uansett årsak, og veiledningen setter naturkatastrofer og strømbrudd ved siden av angrep. En driftshendelse er en uønsket hendelse som etter en vurdering oppfyller organisasjonens kriterier, og verbet veiledningen bruker om den vurderingen, er *erklært*. Definisjonen den bygger på, hentet fra amerikansk føderal lov, dekker en hendelse som faktisk eller overhengende setter konfidensialiteten, integriteten eller tilgjengeligheten til informasjon eller et system i fare, eller som bryter en sikkerhetspolicy.

Sikkerhet og drift bruker ordet med ulikt tyngdepunkt. I sikkerhetsarbeid peker en hendelse som regel mot en motstander, et brudd på en policy eller data som kan ha kommet på avveie. I drift betyr den ethvert uplanlagt avbrudd eller alvorlig forringelse av en tjeneste, uten noen angriper i historien. De to overlapper mer enn ordene antyder: et tjenestenektangrep og en helt vanlig trafikktopp kan se like ut på en graf i starten, og en disk som går full, kan miste data like grundig som en inntrenger.

Nabobegrepene er verdt å holde fra hverandre. En defekt er en feil i produktet; den kan ligge ubemerket i årevis og blir del av en driftshendelse først når den begynner å gjøre skade. Et varsel er en melding om at noe kanskje er galt; mange varsler blir aldri driftshendelser, og mange driftshendelser blir først meldt av en kunde. Praksis for tjenesteforvaltning følger årsaken bak én eller flere hendelser for seg, som et problem.

Bruk begrepet i en beslutning

Bruk «Hva er en driftshendelse?» 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

Avgjørelsen som skjuler seg i ordet, er en terskel. Når slutter en treg side, en underlig innlogging eller en kø som vokser, å være én utviklers sak og blir teamets første prioritet? Legger dere listen for høyt, blir et brudd som sprer seg, behandlet som rutinearbeid av en som ikke kan se det vokse. Legger dere den for lavt, blir folk trukket ut av arbeidet så ofte at det å erklære en driftshendelse slutter å bety noe. Svaret fra NIST er å bli enige om kriteriene før de trengs: driftshendelser erklæres når uønskede hendelser oppfyller kriterier organisasjonen allerede har definert, med kjente falske positiver tatt med i vurderingen. Skrevne kriterier med eksempler er langt billigere enn en diskusjon klokken to om natten.

En erklæring endrer hvem som gjør hva. Én person leder og koordinerer i stedet for å feilsøke, andre blir løst fra det vanlige arbeidet sitt, én kanal bærer fakta, og en logg med tidsstempler starter. Uten det gjør de samme folkene det samme arbeidet i parallell, og den første klare beskrivelsen av problemet er den en kunde skriver.

For noen virksomheter går det også en juridisk klokke. EUs NIS2-direktiv, direktiv (EU) 2022/2555, krever at virksomhetene det omfatter, melder en vesentlig hendelse til nasjonal myndighet: et tidlig varsel innen 24 timer etter at de ble kjent med den, et hendelsesvarsel innen 72 timer og en sluttrapport senest én måned etter hendelsesvarselet. Definisjonen rekker lenger enn angrep, til enhver

hendelse som svekker tilgjengeligheten, autentisiteten, integriteten eller konfidensialiteten til data eller til tjenestene et nettverks- og informasjonssystem tilbyr, så et alvorlig driftsavbrudd kan telle med. Et team som begynner å spørre «er dette en driftshendelse?» på dag to, har allerede brukt opp det første vinduet.

Den løpende kostnaden er folks tid, og den er større enn før. Revisjonen av NISTs veiledning fra 2025 påpeker at hendelser nå skjer ofte, og at gjenopprettingen etter dem ofte tar uker eller måneder, der forgjengeren fra 2012 antok at de var sjeldne og over i løpet av en dag eller to. Å budsjettere for driftshendelser betyr å budsjettere for oppfølgingsarbeidet like mye som for selve natten.

Slik ser det ut i praksis

Én hendelse på dette nettstedet gjelder en skrivebordsapplikasjon for macOS. Diagnoserapportene viste 111 GB komprimerte sider på en maskin med 36 GB den 2026-09-01; en separat stikkprøvemåling av minnebruken viste en vekst på omtrent 41 MB per sekund under en løkke med gjentatte tilkoblingsforsøk som sendte ut core-hendelser. Arbeidet med hendelsen avdekket logghendelser som ble beholdt i en ubegrenset hovedstrøm og kopiert til abonnenter som ikke brukte dem. Bufferne fikk grenser, abonnementer ble filtrert etter hendelsestype, og loggingen fikk et frekvensbudsjett. En sammenligning av fullstendige testkjøringer viste at antallet core-logglinjer falt fra 610 996 til 1 411. Disse målingene gjelder testkjøringen, ikke produksjonstrafikk eller minnebruk etter rettingen. Arkitektursjekker og tester av applikasjonens ressursbudsjett verner om utformingen med faste grenser. Regelen for overfylte buffere kan forkaste gjentatte diagnosehendelser og oppdatere berørt tilstand; separate tidsavbrudd ved avslutning krevde en egen retting.

Andre driftshendelser er av den gjentakende typen. Åtte tunneler med WireGuard og IPsec mellom Google Cloud og Linux-systemer var skjøre og trege å diagnostisere, og en død tunnel kunne bryte kommunikasjonen mellom miljøene. Arbeidet standardiserte konfigurasjonen deres, overvåket helsen deres og gikk løs på de gjentakende problemene med ruting og nøkkelutveksling ved roten i stedet for å starte tunnelene på nytt, og de gjentakende tilkoblingshendelsene opphørte. Når det samme skjer for tredje gang, er det årsaken som er driftshendelsen.

Og noen driftshendelser begynner med at noen prøver å hjelpe. På en plattform uten et administrasjonsverktøy faller det å godkjenne et krav, skjule en omtale eller tømme en cache på en ingeniør med en databasekonsoll, noe prosjektsiden kaller tregt, uten logg og én skrivefeil unna en hendelse. Backoffice-løsningen for operatørene som ble bygd der, rundt 40 adminruter av 128 komponenter, legger det arbeidet bak den samme autorisasjonen og det samme revisjonssporet som resten av produktet, med en løpende kostnad i form av en stor intern flate som må holdes testet og universelt utformet.

Hvor det går galt

Fem personer jobber med den, og ingen leder den. Chatkanalen fylles med teorier, to utviklere ruller tilbake hver sin ting, og kundene hører ingenting på en time, fordi ingen erklærte noe, og dermed fikk ingen jobben med å koordinere. La hvem som helst på teamet erklære en driftshendelse, og gjør det første steget i en erklæring til å utpeke én leder som holder oversikten og loggen.

Den samme driftshendelsen kommer tilbake med noen ukers mellomrom. Innsatsen avsluttes når tjenesten er oppe igjen, og en omstart regnes som løsningen. Behandle det å gjenopprette tjenesten og det å fjerne årsaken som to oppgaver: lukk den første samme natt, og gi den andre en eier og en dato før noen legger seg igjen.

Verktøyene gjør driftshendelsen større. Logging som skriver én linje per hendelse, gir en logg like stor som feilen, og varslingsregler sender hundrevis av varsler for én årsak. Gi logger og varsler et budsjett på forhånd, slå sammen gjentakelser, og test rapporteringsveien under lasten fra den feilen den skal rapportere.

Reparasjonen utløser den neste driftshendelsen. En hastig endring, tastet for hånd mot produksjon, retter ett symptom, starter et nytt problem og etterlater et hull i tidslinjen som gjennomgangen trenger senere. Hold en kort liste over forhåndsgodkjente gjenopprettingstiltak som etterlater et spor, og noter hver endring som gjøres under en driftshendelse.

Lærdommene kommer måneder for sent, eller kommer som skyld. En gjennomgang som holdes etter uker med gjenoppretting, husker lite, og en som spør hvem som gjorde feilen, lærer folk å skjule den neste. Den reviderte veiledningen fra NIST sier at lærdommer ofte bør deles så snart de er identifisert,

og veiledningen om gjenoppretting avsluttes med en etterrapport om hendelsen, tiltakene som ble gjort, og det som ble lært. Skriv ned hva som gjorde feilen lett å gjøre, og endre det.

Les mer

- Incident — definisjonene NISTs publikasjoner bruker, hver vist med loven eller standarden den kommer fra.
- SP 800-61 Rev. 3 — anbefalingene fra NIST om håndtering av hendelser fra 2025, bygd rundt funksjonene i CSF 2.0 i stedet for én enkelt syklus.
- Cybersecurity Framework — rammeverket med funksjonene Govern, Identify, Protect, Detect, Respond og Recover, som veiledningen om hendelser bygger på.
- RFC 2350: Expectations for Computer Security Incident Response — IETFs beste praksis for hva et team for hendelseshåndtering bør publisere om seg selv.

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 en driftshendelse?» 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/