Engineer

Driftshændelse

en hændelse, der bringer et systems data eller drift i fare

Hvad det er

En driftshændelse er en situation, hvor et system i drift har et problem, der er alvorligt nok til, at folk lægger det planlagte arbejde fra sig og tager sig af det med det samme: en tjeneste, der er holdt op med at svare, data, der er blevet ændret, en server, der er løbet tør for hukommelse, eller en konto, som en fremmed bruger. Mange danske it-folk siger bare »incident«, i flertal »incidents«, sikkerhedsfolk taler om en sikkerhedshændelse, og når alt står stille, hedder det et nedbrud. De fleste organisationer sorterer deres hændelser efter alvorlighedsgrad.

På dansk dækker ordet hændelse både det, der bare sker, og det, der kræver handling, og netop derfor er NIST's tredeling nyttig, også uden for sikkerhedsverdenen. Et event er enhver observerbar begivenhed, der involverer it-aktiver: et loginforsøg, en softwareopdatering, en app, der besvarer en forespørgsel. Et negativt event (adverse event) har en skadelig følge, uanset hvad der forårsagede det, og vejledningen stiller naturkatastrofer og strømsvigt side om side med angreb. En driftshændelse er et negativt event, som nogen har vurderet til at opfylde organisationens kriterier, og vejledningens verbum for den vurdering er *erklære*. Den definition, vejledningen hviler på, kommer fra amerikansk føderal lov og dækker en begivenhed, der faktisk eller overhængende bringer fortroligheden, integriteten eller tilgængeligheden af information eller et system i fare, eller som bryder sikkerhedspolitikken.

Sikkerhed og drift bruger ordet med hvert sit tyngdepunkt. I sikkerhedsarbejde forudsætter en hændelse som regel en modstander, et brud på en politik eller data, der måske er sluppet ud af huset. I drift er det enhver uplanlagt afbrydelse eller alvorlig forringelse af en tjeneste, uden at nogen angriber noget. De to overlapper mere, end ordene antyder: et overbelastningsangreb og en almindelig trafiktop kan ligne hinanden på en graf i begyndelsen, og en disk, der løber fuld, kan miste data lige så grundigt som en indtrænger.

Nabobegreberne er værd at holde adskilt. En defekt er en mangel i produktet; den kan ligge upåagtet i årevis og bliver først en del af en driftshændelse, når den begynder at gøre skade. En alarm er en besked om, at noget måske er galt; mange alarmer bliver aldrig til driftshændelser, og mange driftshændelser bliver først meldt af en kunde. I it-servicestyring registrerer man årsagen bag en eller flere hændelser for sig, som et problem.

Brug begrebet i en beslutning

Brug »Hvad er en driftshændelse?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Overvågning og alarmer, der siger til, mens fejlen stadig er lille, og tallene, der viser, hvor tit den bliver ved med at være det.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har bygget det første observerbarhedsdashboard — virksomhedens første overblik over sine egne systemer

Har bygget det første observerbarhedsdashboard Kontakt os →

Hvorfor det betyder noget

Bag ordet gemmer sig en tærskel. Hvornår holder en langsom side, et mærkeligt login eller en voksende kø op med at være én udviklers sag og bliver teamets første prioritet? Lægges barren for højt, bliver et brud, der breder sig, behandlet som rutinearbejde af en, der ikke kan se det vokse. Lægges den for lavt, bliver folk revet ud af deres arbejde så tit, at det mister sin betydning at erklære noget. NIST's svar er at aftale kriterierne, før der er brug for dem: driftshændelser erklæres, når negative events opfylder kriterier, som organisationen allerede har fastlagt, og kendte falske positiver indgår i vurderingen. Nedskrevne kriterier med eksempler er langt billigere end en diskussion klokken to om natten.

En erklæring ændrer, hvem der gør hvad. Én person leder og koordinerer i stedet for at fejlsøge, andre bliver fritaget for deres normale opgaver, én kanal bærer fakta, og en log med tidsstempler går i gang. Uden den laver de samme folk det samme arbejde hver for sig, og den første klare beskrivelse af problemet er den, en kunde skriver.

For nogle virksomheder tikker der også et juridisk ur. EU's NIS2-direktiv, direktiv (EU) 2022/2555, pålægger de organisationer, det omfatter, at indberette en væsentlig hændelse til den nationale myndighed: en tidlig varsling inden for 24 timer efter, at de er blevet opmærksomme på den, en hændelsesunderretning inden for 72 timer og en endelig rapport senest en måned efter underretningen. Direktivets definition rækker ud over angreb til enhver begivenhed, der

kompromitterer tilgængeligheden, ægtheden, integriteten eller fortroligheden af data eller af de tjenester, et net- og informationssystem leverer, så et alvorligt nedbrud kan tælle med. Et team, der først på andendagen spørger »er det her en driftshændelse?«, har allerede brugt det første vindue.

Den løbende pris er folks tid, og den er vokset. Den reviderede udgave af NIST's vejledning fra 2025 konstaterer, at hændelser nu sker ofte, og at genopretningen tit tager uger eller måneder, hvor forgængeren fra 2012 gik ud fra, at de var sjældne og overstået på en dag eller to. Et budget for driftshændelser skal derfor dække opfølgningen og ikke kun selve natten.

Sådan ser det ud i praksis

En hændelse på dette site vedrører et skrivebordsprogram til macOS. Dets diagnoserapporter registrerede 111 GB komprimerede sider på en maskine med 36 GB den 2026-09-01; en separat måling af hukommelsesforbruget registrerede en vækst på omkring 41 MB i sekundet under en løkke, som gentog forbindelsesforsøg og udsendte core-hændelser. Gennemgangen fandt loghændelser beholdt i en ubegrænset hovedstrøm og kopieret til abonnenter, der ikke brugte dem. Bufferne blev afgrænset, abonnementerne filtreret efter hændelsestype, og logningen fik et hastighedsbudget. En sammenligning af fulde testkørsler registrerede et fald fra 610.996 core-loglinjer til 1.411. De målinger vedrører testkørslen, ikke produktionstrafik eller hukommelsesforbrug efter rettelsen. Arkitekturkontroller og tests af applikationens budgetter understøtter det afgrænsede design. Dets politik for bufferoverløb kan kassere gentagne diagnostiske hændelser og genindlæse den berørte tilstand; separate timeouts ved nedlukning krævede deres egen rettelse.

Andre driftshændelser er af den tilbagevendende slags. Otte WireGuard- og IPsec-tunneler mellem Google Cloud og Linux-systemer var skrøbelige og langsomme at fejlsøge, og en tunnel, der var nede, kunne afbryde forbindelsen mellem miljøerne. Arbejdet ensrettede konfigurationen, overvågede tunnelernes tilstand og gik til roden af de gentagne problemer med routing og nøgleudveksling i stedet for at genstarte, og forbindelsesproblemerne holdt op med at komme igen. Når det samme sker for tredje gang, er årsagen selve hændelsen.

Og nogle driftshændelser begynder med, at nogen prøver at hjælpe. På en platform uden admin-værktøj lander opgaver som at godkende et ejerskabskrav, skjule en anmeldelse eller rydde en cache hos en udvikler med en

databasekonsol, hvor intet bliver logget, og hvor en enkelt tastefejl kan blive til en driftshændelse. Back-officen, der blev bygget til platformen, omkring 40 admin-ruter af 128 komponenter, lægger det arbejde bag den samme autorisation og det samme revisionsspor som resten af produktet, til en løbende pris: en stor intern flade, der skal holdes testet og tilgængelig.

Hvor det går galt

Fem personer arbejder på sagen, og ingen leder den. Chatkanalen fyldes med teorier, to udviklere ruller hver sin ændring tilbage, og kunderne hører ingenting i en time, fordi ingen erklærede hændelsen, og derfor fik ingen til opgave at koordinere. Lad alle i teamet erklære, og gør det til første skridt at udpege én leder, der holder overblikket og loggen.

Den samme hændelse vender tilbage med få ugers mellemrum. Indsatsen slutter, når tjenesten kører igen, og en genstart tæller som rettelsen. Behandl genopretning af tjenesten og fjernelse af årsagen som to opgaver: luk den første samme nat, og giv den anden en ejer og en dato, før nogen går i seng igen.

Værktøjerne gør hændelsen større. Logning, der skriver en linje pr. event, giver en log, der er lige så stor som fejlen, og alarmregler sender hundredvis af beskeder om én årsag. Giv logs og alarmer et budget på forhånd, slå gentagelser sammen, og test rapporteringsvejen under den belastning, som fejlen selv giver.

Reparationen udløser den næste hændelse. En hastig ændring, tastet i hånden mod produktion, fjerner ét symptom, starter et nyt problem og efterlader et hul i den tidslinje, gennemgangen senere skal bruge. Hav en kort liste over godkendte genopretningshandlinger, der efterlader et spor, og noter hver ændring, der laves under hændelsen.

Erfaringerne kommer måneder for sent eller som skyld. En gennemgang, der holdes efter ugers genopretning, husker lidt, og en gennemgang, der spørger, hvem der begik fejlen, lærer folk at skjule den næste. NIST's reviderede vejledning siger, at erfaringer ofte bør deles, så snart de er identificeret, og dens anbefalinger om genopretning slutter med en rapport om hændelsen, de handlinger, der blev taget, og det, man lærte. Skriv ned, hvad der gjorde fejlen let at begå, og lav det om.

Læs mere

- Incident — de definitioner, NIST's publikationer bruger, hver med den lov eller standard, den stammer fra.
- SP 800-61 Rev. 3 — NIST's anbefalinger til hændelseshåndtering fra 2025, bygget op om funktionerne i CSF 2.0 i stedet for én fast cyklus.
- Cybersecurity Framework — rammeværket med funktionerne Govern, Identify, Protect, Detect, Respond og Recover, som vejledningen følger.
- RFC 2350: Expectations for Computer Security Incident Response — IETF's anbefalede praksis for, hvad et beredskabsteam bør offentliggøre om sig selv.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er en driftshændelse?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/incident/