Engineer

Incident

en händelse som sätter ett systems data eller tjänst på spel

Vad det är

En incident är en händelse som stör en tjänst eller sätter systemets data på spel och behöver hanteras skyndsamt. När kunder plötsligt inte kan betala i en nätbutik kan det vara en driftincident. Ett stulet konto kan behöva hanteras som en säkerhetsincident även när webbplatsen fungerar som vanligt. Många organisationer har därför kriterier som avgör när teamet ska agera och hur allvarlig en incident är.

NIST:s vägledning för incidenthantering drar gränsen i tre steg, och de håller långt utanför säkerhetsarbetet. En händelse är allt observerbart som rör it-tillgångar: ett inloggningsförsök, en programuppdatering, en app som besvarar en begäran. En negativ händelse är en händelse med en skadlig följd, oavsett orsak, och vägledningen ställer naturkatastrofer och strömavbrott bredvid angrepp. En incident är en negativ händelse som någon har bedömt uppfyller organisationens kriterier, och vägledningens verb för den bedömningen är *declared*, deklarerad. Definitionen som den vilar på, hämtad ur amerikansk federal lag, omfattar det som faktiskt eller omedelbart sätter konfidentialitet, riktighet eller tillgänglighet hos information eller ett system på spel, eller som bryter mot en säkerhetspolicy.

Säkerhet och drift använder ordet med olika tyngdpunkt. I säkerhetsarbete antyder en incident oftast en motståndare, ett policybrott eller data som kan ha lämnat huset. I drift betyder den varje oplanerat avbrott eller allvarlig försämring av en tjänst, utan någon angripare i historien. De två överlappar mer än orden antyder: en överbelastningsattack och en vanlig trafiktopp kan se likadana ut i en graf till en början, och en disk som blir full kan förlora data lika grundligt som en inkräktare.

Grannorden är värda att hålla isär. En defekt är en brist i produkten; den kan ligga obemärkt i åratal och blir en del av en incident först när den börjar göra skada. Ett larm är ett meddelande om att något kan vara fel; många larm blir aldrig incidenter, och många incidenter rapporteras först av en kund. Inom tjänstehantering följs orsaken bakom en eller flera incidenter upp för sig, som ett problem.

Använd begreppet i ett beslut

Använd ”Vad är en incident?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Övervakning och larm som säger till medan ett fel fortfarande är litet, och siffrorna som visar hur ofta det förblir så.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Byggde företagets första observerbarhetsdashboard — företagets första överblick över de egna systemen

Byggde företagets första observerbarhetsdashboard Hör av er →

Varför det spelar roll

Beslutet som gömmer sig i ordet är en tröskel. När slutar en långsam sida, en udda inloggning eller en växande kö att vara en enskild ingenjörs ärende och blir teamets första prioritet? Lägg ribban för högt, och ett intrång som sprider sig hanteras som rutinarbete av någon som inte kan se det växa. Lägg den för lågt, och folk dras bort från sitt arbete så ofta att en deklaration slutar betyda något. NIST:s svar är att komma överens om kriterierna innan de behövs: incidenter deklareras när negativa händelser uppfyller kriterier som organisationen redan har definierat, med kända falsklarm inräknade. Skrivna kriterier med exempel är betydligt billigare än en diskussion klockan två på natten.

En deklaration ändrar vem som gör vad. En person leder och samordnar i stället för att felsöka, andra frigörs från sitt vanliga arbete, en kanal bär fakta och en logg med tidsstämplar startar. Utan det gör samma personer samma arbete parallellt, och det första tydliga beskedet om problemet blir det som en kund skriver.

För en del företag finns också en klocka i lagen. EU:s NIS2-direktiv, direktiv (EU) 2022/2555, kräver att organisationer som omfattas rapporterar betydande incidenter till en nationell incidenthanteringsenhet (CSIRT) eller behörig myndighet. Som huvudregel lämnar de en tidig varning inom 24 timmar och en incidentanmälan inom 72 timmar efter att de fått kännedom om incidenten. Slutrapporten lämnas normalt senast en månad efter incidentanmälan.

Direktivets definition sträcker sig bortom angrepp till varje händelse som äventyrar tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos data eller hos de tjänster som ett nätverks- och informationssystem erbjuder, så ett allvarligt driftstopp kan räknas. Ett team som börjar fråga ”är det här en incident?” på andra dagen har redan förbrukat det första fönstret.

Den löpande kostnaden är människors tid, och den är större än den brukade vara. 2025 års revision av NIST:s vägledning konstaterar att incidenter numera inträffar ofta och att återhämtningen ofta tar veckor eller månader, medan föregångaren från 2012 utgick från att de var sällsynta och över inom en dag eller två. Att budgetera för incidenter betyder att budgetera för efterarbetet lika mycket som för själva natten.

Så ser det ut i praktiken

Ett fall i portföljen gäller en skrivbordsapp för macOS. Dess diagnostikrapporter registrerade 111 GB komprimerade sidor på en maskin med 36 GB den 2026-09-01; ett separat stickprov av minnesförbrukningen registrerade en ökning med ungefär 41 MB per sekund under en återförsöksslinga för anslutningen som skickade core-händelser. Genomgången fann logghändelser som behölls i en obegränsad huvudström och kopierades till prenumeranter som inte använde dem. Buffertarna begränsades, prenumerationerna filtrerades efter händelsetyp och loggningen fick en taktbudget. En jämförelse av fullständiga testkörningar registrerade att 610 996 core-loggrader blev 1 411. De mätningarna gäller testkörningen, inte produktionstrafik eller minnesförbrukning efter korrigeringen. Arkitekturkontroller och tester av applikationens budgetar skyddar den begränsade designen. Dess policy för buffertöverflöde kan kasta bort upprepade diagnostiska händelser och läsa in berört tillstånd på nytt; separata tidsgränser vid avstängning behövde en egen korrigering.

Andra incidenter är av det återkommande slaget. Åtta tunnlar med WireGuard och IPsec mellan Google Cloud och Linux-system var bräckliga och långsamma att diagnostisera, och en död tunnel kunde bryta kommunikationen mellan miljöerna. Arbetet standardiserade konfigurationen, övervakade tunnlarnas tillstånd och åtgärdade de återkommande problemen med routning och nyckelutbyte vid roten i stället för att starta om tunnlarna, och de återkommande anslutningsincidenterna upphörde. När samma sak händer för tredje gången är orsaken själva incidenten.

Och vissa incidenter börjar med att någon försöker hjälpa till. På en plattform utan administrationsverktyg hamnar det på en ingenjör med en databaskonsol att godkänna ett anspråk, dölja en recension eller rensa en cache, något som projektsidan kallar långsamt, ologgat och ett skrivfel från en incident. Det backoffice för operatörer som byggdes där, ungefär 40 admin-routes byggda av 128 komponenter, lägger det arbetet bakom samma auktorisering och samma revisionsspår som resten av produkten, till den löpande kostnaden av en stor intern yta att hålla testad och tillgänglig.

Var det går fel

Fem personer arbetar med den och ingen leder den. Chattkanalen fylls av teorier, två ingenjörer rullar tillbaka olika saker, och kunderna hör ingenting på en timme, eftersom ingen deklarerade incidenten, och därmed fick ingen i uppdrag att samordna. Låt vem som helst i teamet deklarera, och gör det första steget i varje deklaration till att utse en ledare som håller helhetsbilden och loggen.

Samma incident kommer tillbaka med några veckors mellanrum. Insatsen slutar när tjänsten är uppe igen, och en omstart räknas som lösningen. Behandla återställd tjänst och borttagen orsak som två uppgifter: stäng den första under natten, och ge den andra en ägare och ett datum innan någon går och lägger sig.

Verktygen gör incidenten större. Loggning som skriver en rad per händelse ger en logg lika stor som felet, och larmregler skickar hundratals aviseringar för en enda orsak. Ge loggar och larm en budget i förväg, slå ihop upprepningar och testa rapporteringsvägen under lasten från det fel som den rapporterar.

Lagningen orsakar nästa incident. En hastig ändring som skrivs för hand mot produktion lagar ett symtom, startar ett annat problem och lämnar ett hål i tidslinjen som genomgången senare behöver. Håll en kort lista med förhandsgodkända återställningsåtgärder som lämnar spår, och skriv ned varje ändring som görs under en incident.

Lärdomarna kommer månader för sent, eller kommer som skuld. En genomgång som hålls efter veckor av återhämtning minns lite, och en som frågar vem som gjorde misstaget lär folk att dölja nästa. NIST:s reviderade vägledning säger att lärdomar ofta bör delas så snart de har identifierats, och dess vägledning för återhämtning slutar med en rapport efter insatsen om incidenten, de åtgärder som vidtogs och vad man lärde sig. Skriv ned vad som gjorde misstaget lätt att begå, och ändra det.

Läs mer

- Incident — de definitioner som NIST:s publikationer använder, var och en med den lag eller standard den kommer från.
- SP 800-61 Rev. 3 — NIST:s rekommendationer för incidenthantering från 2025, byggda kring funktionerna i CSF 2.0 i stället för en enda insatscykel.
- Cybersecurity Framework — ramverket med funktionerna Govern, Identify, Protect, Detect, Respond och Recover, som incidentvägledningen bygger på.
- RFC 2350: Expectations for Computer Security Incident Response — IETF:s bästa praxis för vad ett incidentteam bör publicera om sig självt.
- NIS2-direktivet, artikel 23 anger vem som ska underrättas, huvudregeln för tidsfristerna och vad som gäller vid undantag.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är en incident?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/incident/