Engineer

Інцидент

подія, що ставить під загрозу дані чи роботу системи

Що це таке

Інцидент — це проблема в робочій системі, настільки серйозна, що люди відкладають заплановану роботу й беруться за неї негайно: сервіс перестав відповідати, записи хтось змінив, на сервері скінчилася пам'ять, обліковим записом користується стороння особа. Фахівці з безпеки кажуть «інцидент безпеки», експлуатаційники — «інцидент у продакшні» або просто «збій» чи «аварія», і більшість організацій розкладає свої інциденти за рівнями серйозності.

Настанови NIST із реагування на інциденти проводять межу в три кроки, і цей поділ працює не лише в безпеці. Подія — це будь-яке спостережуване явище, пов'язане з IT-активами: спроба входу, оновлення програмного забезпечення, відповідь застосунку на запит. Несприятлива подія має негативні наслідки, хоч би що її спричинило, і настанови ставлять стихійні лиха та перебої з електроживленням поруч з атаками. Інцидент — це несприятлива подія, яку хтось визнав такою, що відповідає критеріям організації, і для цього рішення настанови вживають дієслово *оголосити*. Визначення, на яке вони спираються, взято з федерального законодавства США: це подія, яка фактично або неминуче ставить під загрозу конфіденційність, цілісність чи доступність інформації або системи, або порушує політику безпеки.

Безпека й експлуатація вживають це слово з різними акцентами. У сфері безпеки інцидент зазвичай передбачає зловмисника, порушення політики або дані, які, можливо, вже опинилися за межами компанії. В експлуатації це будь-яке незаплановане переривання чи серйозне погіршення сервісу, де ніхто нічого не атакує. Ці два світи перетинаються більше, ніж підказує термінологія: DoS-атака і звичайний сплеск трафіку спершу можуть виглядати на графіку однаково, а диск, що заповнився, здатен знищити дані не гірше за зловмисника.

Сусідні терміни варто розрізняти. Дефект — це вада продукту; він може роками лишатися непоміченим і стає частиною інциденту лише тоді, коли починає шкодити. Тривога — це повідомлення про те, що щось, можливо, пішло не так; багато тривог так і не переростають в інциденти, а про багато інцидентів першим повідомляє клієнт. У практиці керування IT-послугами причину одного чи кількох інцидентів обліковують окремо, як проблему.

Застосуйте поняття до рішення

Застосуйте «Що таке інцидент?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Моніторинг і сповіщення, які попереджають, поки збій ще малий, і цифри, що показують, як часто так і залишається.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Запустила перший дашборд спостережуваності — перший огляд власних систем компанії

Запустила перший дашборд спостережуваності Зв'язатися з нами →

Чому це важливо

У самому слові захований поріг. У який момент повільна сторінка, дивний вхід у систему чи черга, що росте, перестають бути завданням одного інженера й стають першим пріоритетом команди? Якщо планку поставити зависоко, злам, що розростається, розбиратиме як рутинну справу людина, яка не бачить, як він шириться. Якщо занизько, людей відривають від роботи так часто, що оголошення інциденту втрачає вагу. NIST радить домовитися про критерії заздалегідь: інциденти оголошують, коли несприятливі події відповідають уже визначеним критеріям організації, з урахуванням відомих хибнопозитивних спрацювань. Записані критерії з прикладами обходяться значно дешевше, ніж суперечка о другій ночі.

Оголошення змінює розподіл ролей. Одна людина керує й координує, а не налагоджує, інших звільняють від звичайної роботи, факти йдуть одним каналом, і починається журнал із часовими позначками. Без цього ті самі люди паралельно роблять ту саму роботу, а перший чіткий опис проблеми пише клієнт.

Для деяких компаній цокає ще й юридичний годинник. Директива ЄС NIS2, Директива (ЄС) 2022/2555, зобов’язує організації, на які поширюється, повідомляти національний орган про значний інцидент: раннє попередження — протягом 24 годин після того, як про нього стало відомо, повідомлення про інцидент — протягом 72 годин, остаточний звіт — не

пізніше ніж через місяць після цього повідомлення. Її визначення виходить за межі атак і охоплює будь-яку подію, що порушує доступність, автентичність, цілісність або конфіденційність даних чи послуг мережевих та інформаційних систем, тож серйозний збій теж може під нього підпадати. Команда, яка лише на другий день питає «а це інцидент?», уже змарнувала перше вікно.

Постійна ціна — час людей, і вона зросла. Переглянута редакція настанов NIST 2025 року констатує, що інциденти тепер стаються часто, а відновлення після них нерідко триває тижні або місяці, тоді як попередня редакція 2012 року виходила з того, що вони рідкісні й минають за день-два. Тож бюджет на інциденти має покривати й подальшу роботу, а не лише саму ніч.

Як це виглядає на практиці

Один з описаних на цьому сайті інцидентів стосується настільного застосунку macOS. Його діагностичні звіти зафіксували 111 ГБ стиснутих сторінок на машині з 36 ГБ 2026-09-01; окремий замір обсягу зайнятої пам’яті зафіксував зростання приблизно на 41 МБ за секунду під час циклу повторних спроб підключення, що генерував події ядра програми. Під час реагування виявлено події журналу, які зберігалися в необмеженому основному потоці й копіювалися підписникам, що їх не використовували. Буфери обмежили, підписки відфільтрували за типом події, а журналюванню надали бюджет частоти записів. Порівняння повних тестових запусків зафіксувало скорочення 610 996 рядків журналу ядра програми до 1 411. Ці вимірювання стосуються тестового запуску, а не виробничого трафіку чи використання пам’яті після виправлення. Архітектурні перевірки й тести бюджетів застосунку перевіряють дотримання обмежень у цій схемі. Її політика переповнення може відкидати повторювані діагностичні події й оновлювати відповідний стан; окремі тайм-аути під час завершення роботи потребували власного виправлення.

Інші інциденти повторюються. Вісім тунелів WireGuard та IPsec між Google Cloud і Linux-системами були крихкими й повільно піддавалися діагностиці, а тунель, що впав, міг обірвати зв’язок між середовищами. Конфігурацію уніфікували, стан тунелів почали відстежувати, а збої маршрутизації та обміну ключами, що поверталися знову й знову, перестали гасити перезапуском і розібрали до першопричини, після чого зв’язок перестав регулярно обриватися. Коли те саме стається втретє, інцидентом є сама причина.

А деякі інциденти починаються зі спроби допомогти. На платформі без адміністративного інструмента схвалити заявку на володіння, приховати відгук чи очистити кеш доводиться інженерові в консолі бази даних, де дії не потрапляють у журнал і одна описка може обернутися інцидентом. Бек-офіс, створений для цієї платформи, — близько 40 адміністративних маршрутів зі 128 компонентів — проводить цю роботу через ту саму авторизацію й той самий журнал аудиту, що й решту продукту, ціною великої внутрішньої поверхні, яку постійно треба тримати протестованою й доступною.

Де виникають проблеми

П’ятеро людей працюють над інцидентом, і ніхто ним не керує. Чат заповнюється гіпотезами, двоє інженерів відкочують різні зміни, а клієнти годину нічого не чують, бо ніхто не оголосив інцидент, отже, ніхто й не отримав завдання координувати. Дозвольте будь-кому в команді оголошувати інцидент і зробіть першим кроком призначення одного керівника, який тримає загальну картину та журнал.

Той самий інцидент повертається кожні кілька тижнів. Реагування закінчується, щойно сервіс знову працює, а перезапуск вважають виправленням. Розглядайте відновлення сервісу й усунення причини як два окремі завдання: перше закрийте тієї ж ночі, а другому призначте відповідального й термін, перш ніж хтось піде спати.

Інструменти роздмухують інцидент. Журналювання, яке пише рядок на кожну подію, дає журнал завбільшки з саму несправність, а правила тривог шлють сотні сповіщень через одну причину. Заздалегідь задайте бюджет журналам і тривогам, згортайте повтори й перевіряйте канал звітування під тим навантаженням, яке створює сама несправність.

Ремонт спричиняє наступний інцидент. Поспішна зміна, введена вручну просто на продакшні, прибирає один симптом, запускає нову проблему й лишає діру в хронології, потрібній для подальшого розбору. Майте короткий перелік заздалегідь погоджених дій із відновлення, які залишають слід, і фіксуйте кожну зміну, внесену під час інциденту.

Висновки надходять на місяці пізніше або у вигляді звинувачень. Розбір, проведений після тижнів відновлення, мало що пам’ятає, а розбір, що шукає винного, вчить людей приховувати наступну помилку. Переглянуті настанови NIST радять здебільшого ділитися висновками одразу, щойно їх

виявлено, а їхні рекомендації щодо відновлення завершуються звітом про інцидент, ужиті заходи та здобуті уроки. Запишіть, що зробило помилку легкою, і змініть саме це.

Що почитати далі

- Incident — визначення, якими користуються публікації NIST, кожне з посиланням на закон чи стандарт, звідки його взято.
- SP 800-61 Rev. 3 — рекомендації NIST 2025 року щодо реагування на інциденти, побудовані навколо функцій CSF 2.0, а не єдиного циклу реагування.
- Cybersecurity Framework — рамкова модель із функціями Govern, Identify, Protect, Detect, Respond і Recover, на які спираються настанови.
- RFC 2350: Expectations for Computer Security Incident Response — найкраща чинна практика IETF щодо того, що команда реагування на інциденти має публікувати про себе.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке інцидент?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/incident/