Engineer

Інформаційна безпека

захист даних і систем від зловживань і шкоди

Що це таке

Інформаційна безпека — це робота з того, щоб інформація та системи, які її зберігають і передають, залишалися в тому стані, якого хочуть їхні власники: її читають лише ті, кому належить, змінюють лише так, як було задумано, і вона доступна, коли потрібна. У щоденній мові й у більшості назв посад кажуть просто «безпека». Визначення в глосарії NIST походить із федерального закону США, 44 U.S.C. 3552, який називає три властивості. Конфіденційність зберігає дозволені обмеження доступу та розголошення. Цілісність захищає від неналежної зміни чи знищення і включає змогу довести, що інформація справжня і що її відправник не може правдоподібно заперечити, що надіслав її. Доступність означає своєчасний і надійний доступ до інформації та можливість нею користуватися.

Ці три властивості тягнуть у різні боки, і саме ця напруга робить роботу складною. База даних, до якої ніхто не може дістатися, ідеально конфіденційна й нікому не потрібна. Резервна копія, що лежить у трьох місцях, покращує доступність і дає злодієві три місця для пошуку. Більшість рішень у цій галузі стосується того, де стати між цими трьома силами для одного конкретного виду інформації, і відповідь для публічного прайс-листа зовсім інша, ніж для медичної картки пацієнта.

Роботу виконують через засоби контролю, кожен з яких — конкретний захід із конкретною метою. Одні технічні: шифрування, автентифікація, брандмауер, контроль доступу. Інші процедурні: перевірка перед випуском зміни, правило, що працівник, який звільняється, втрачає доступ в останній робочий день, письмовий план на випадок інциденту. Ще інші фізичні, як-от замкнена кімната. NIST SP 800-53 — це каталог таких засобів, згрупованих у родини й описаних так, щоб організація могла вибрати ті, що відповідають її

ризикам. NIST Cybersecurity Framework 2.0 працює на рівень вище. Він описує результати в шести функціях, Govern, Identify, Protect, Detect, Respond і Recover, і прямо зазначає, що не приписує, як саме цих результатів досягати.

Застосуйте поняття до рішення

Застосуйте «Що таке інформаційна безпека?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

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. Написала 1 000 правил RBAC для Linux-серверів — 1,000 правил доступу написано, щоб усунути вразливість

Написала 1 000 правил RBAC для Linux-серверів Зв'язатися з нами →

Чому це важливо

Шкоду інформації важко виправити. Дані, які витекли, залишаються такими, хоч би що полагодили потім. Запис, який змінили так, що ніхто не помітив, ставить під сумнів кожне пізніше рішення, яке на нього спиралося. Збій у день нарахування зарплати чи в останній день подання тендерної пропозиції коштує більше, ніж години, які він триває. Першими зазвичай платять ті, чиї це були дані, а компанія, яка їх зберігала, — уже потім.

Для покупця складність у тому, що безпеку не видно, поки вона працює. Два постачальники можуть перелічити ті самі інструменти тими самими словами, і, можливо, лише один із них перевірив, що ці інструменти роблять те, що написано в переліку. Тому корисні запитання стосуються доказів: які засоби контролю є, звідки хтось знає, що вони працюють сьогодні, а не лише в день встановлення, і що відбувається, коли один із них повідомляє про проблему? Постачальник, який відповідає звітом, згенерованим із робочої системи, стоїть в іншому становищі, ніж той, хто відповідає документом про політику.

Компроміси справжні, і стосуються вони здебільшого часу й незручностей. Кожен сканер дає знахідки, і кожна знахідка потребує людини, яка вирішить, чи вона важлива. Кожен додатковий крок під час входу — це крок, який люди шукатимуть, як обійти. Кожен доданий засіб контролю треба підтримувати, інакше він тихо стає засобом, що існує лише на папері. Функція Govern відкриває цю рамкову модель, бо це управлінські рішення не менше, ніж технічні: хтось має вирішити, який ризик прийнятний, які дані заслуговують на найбільшу увагу і скільки може коштувати решта захисту.

Як це виглядає на практиці

Ловити проблеми, щойно вони з'являються, — завдання безперервної програми безпеки для платформи застосунку. Статичний аналіз виконує CodeQL, динамічне тестування — ZAP, а залежності Go перевіряє govulncheck. Перелік програмних компонентів (SBOM) генерується під час кожної збірки за допомогою Anchore та Syft, Gitleaks шукає в історії облікові дані, кожна сторонння GitHub Action закріплена за хешем коміту, а Dependabot стежить за 6 екосистемами. Автоматизацію доповнює 21 письмовий аудит безпеки, зокрема модель загроз і оцінка за посібником з тестування OWASP. Вразливість, яку розпізнають налаштовані перевірки, може зупинити збірку. Сторінка прямо називає ціну: обсяг знахідок і постійний розбір, потрібний, щоб сигнал лишався корисним.

Чесний опис робочої системи дають сім ролей лише для читання, які описують робочий хост у Markdown, побудовані тому, що стек метрик не вміщується в 464 МБ хоста. Звіт про доступ охоплює облікові записи, межі sudo, відбитки ключів, користувачів git-сервера і ролі бази даних. Звіт з безпеки відповідає, чи посилення захисту справді діє, а не лише налаштоване, і виводить правила брандмауера в порядку зіставлення та чинний набір правил блокування. Звіт не друкує жодного числа, якого прогін не виміряв. Серед іншого, звіти знайшли два мертві засоби безпеки й незадекларований порт у режимі прослуховування.

Перевіряти, що засіб контролю справді діє, варто тому, що той самий хост цілий рік працював з обмеженням частоти, яке стояло нижче ширшого правила, що спрацьовувало першим, тож до нього не дійшов жоден пакет. Тепер перевірки читають нумерований перелік правил і живий ланцюжок фільтра та звіряють саме порядок. На кожен порт — рівно одне правило, завжди із зазначеним протоколом, на порту SSH стоїть обмеження частоти і ніколи — дозвіл поруч із ним, а оголошену публічну поверхню з п'яти портів звіряють цілком.

Де виникають проблеми

Засіб контролю налаштований, але так і не діє. Параметр у файлі, правило в списку чи політика у вікі фіксують те, що хтось задумав. Лише перевірка робочої системи показує, як є насправді. Програма, яка рахує засоби контролю замість того, щоб їх тестувати, звітує про повне покриття, поки прогалини стоять відкритими, і першу справжню перевірку проводить хтось ззовні.

Усе тримається на одному шарі. Міцний периметр із широко відкритим доступом за ним означає, що одна помилка віддає все. Ешелонований захист виходить із того, що кожен шар колись підведе, і ставить за ним наступний, тож украдений пароль ще зустріне другий фактор, а скомпрометований сервіс — вузьку роль у базі даних.

Знахідки надходять швидше, ніж їх хтось читає. Сканер, який повідомляє про кожну можливу проблему з однаковою терміновістю, привчає людей перестати його читати. Чіткі власники, пороги серйозності й письмове правило, коли знахідка зупиняє випуск, зберігають цінність результату.

Про доступність згадують лише під час збою. Конфіденційність отримує найбільше уваги, бо витоки потрапляють у новини. Резервні копії, які ніколи не відновлювали, єдиний сервер без плану заміни і сертифікати, що непомітно спливають, — усе це підводить третю властивість, і зазвичай у найгірший можливий день.

Сторонні люди не мають очевидного місця, куди повідомити про проблему. Той, хто знаходить слабке місце в публічному сервісі, має знати, куди про це написати. RFC 9116 визначає файл security.txt, який віддають за адресою /.well-known/security.txt, з обов'язковим полем Contact, що вказує, куди надсилати повідомлення, і обов'язковим полем Expires, що вказує, як довго файлу можна довіряти. Без нього повідомлення потрапляють у загальну скриньку або до того, хто відповість першим.

Що почитати далі

- Information security у глосарії NIST CSRC — визначення з FIPS 200 і 44 U.S.C. 3552 із трьома властивостями.
- 44 U.S.C. 3552 — закон, що визначає конфіденційність, цілісність і доступність.
- NIST SP 800-53 Rev. 5 — каталог засобів контролю безпеки та приватності, згрупованих у родини.
- NIST Cybersecurity Framework 2.0 — шість функцій, що описують результати безпеки, від Govern до Recover.
- RFC 9116 — формат security.txt, який підказує дослідникам, куди повідомляти про вразливість.

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 інформаційна безпека?» 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/security/