Engineer

Informationssäkerhet

skydd av data och system mot missbruk och skada

Vad det är

Informationssäkerhet handlar om att hålla information, och de system som lagrar och flyttar den, i det skick som ägarna avser: läst bara av dem som ska läsa den, ändrad bara på de sätt som var tänkta, och på plats när den behövs. I vardagligt tal, och i de flesta jobbtitlar, kortas ordet till säkerhet. Definitionen i ordlistan från NIST kommer från amerikansk federal lag, 44 U.S.C. 3552, som namnger tre egenskaper. Konfidentialitet upprätthåller beslutade begränsningar av åtkomst och utlämnande. Riktighet, på engelska integrity, skyddar mot otillbörlig ändring eller förstörelse och omfattar att kunna visa att informationen är äkta och att avsändaren inte trovärdigt kan förneka att den skickades. Tillgänglighet betyder snabb och pålitlig åtkomst till informationen och möjlighet att använda den.

De tre drar åt olika håll, och den spänningen är det mesta av det som gör arbetet svårt. En databas som ingen kan nå är fullständigt konfidentiell och till nytta för ingen. En säkerhetskopia som förvaras på tre ställen förbättrar tillgängligheten och ger en tjuv tre ställen att leta på. De flesta beslut inom området handlar om var man ska placera sig mellan de krafterna för en viss sorts information, och svaret för en offentlig prislista ser helt annorlunda ut än svaret för en patients journal.

Arbetet görs med säkerhetsåtgärder, var och en ett bestämt skydd med ett bestämt syfte. En del är tekniska: kryptering, autentisering, en brandvägg, åtkomstkontroll. En del är organisatoriska: en granskning innan en ändring levereras, en regel om att den som slutar förlorar sin åtkomst på sista arbetsdagen, en skriven plan för en incident. En del är fysiska, som ett låst rum. NIST SP 800-53 är en katalog över sådana åtgärder, ordnade i familjer och skrivna så att en organisation kan välja dem som passar dess risker. NIST Cybersecurity Framework 2.0 arbetar en nivå högre. Det beskriver önskade utfall under sex funktioner, Govern, Identify, Protect, Detect, Respond och Recover, och säger uttryckligen att det inte föreskriver hur utfallen ska uppnås.

Använd begreppet i ett beslut

Använd ”Vad är informationssäkerhet?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

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. Skrev 1 000 RBAC-regler som säkrar Linux-servrar — 1,000 åtkomstregler, skrivna för att täppa till en säkerhetslucka

Skrev 1 000 RBAC-regler som säkrar Linux-servrar Hör av er →

Varför det spelar roll

Skada på information är svår att göra ogjord. Data som har läckt förblir läckt, vad som än rättas efteråt. En post som ändrades utan att någon märkte det gör varje senare beslut som byggde på den tvivelaktigt. Ett avbrott den dag då en lönekörning eller en anbudsfrist infaller kostar mer än de timmar det varar. De människor vars data det var bär oftast kostnaden först, och företaget som förvaltade datan i andra hand.

För en köpare är det svåra att säkerheten är osynlig så länge den fungerar. Två leverantörer kan lista samma verktyg med samma ord, och kanske har bara den ena kontrollerat att verktygen gör det listan påstår. De användbara frågorna handlar därför om belägg: vilka åtgärder som finns på plats, hur någon vet att de fungerar i dag och inte bara den dag de installerades, och vad som händer när en av dem rapporterar ett problem. En leverantör som svarar med en rapport genererad ur systemet i drift står i ett annat läge än en som svarar med ett policydokument.

Avvägningarna är verkliga, och de handlar mest om tid och friktion. Varje skanner ger fynd, och varje fynd kräver att en människa avgör om det spelar någon roll. Varje extra steg vid inloggningen är ett steg som folk kommer att leta efter vägar runt. Varje åtgärd som läggs till måste underhållas, annars blir den i tysthet en åtgärd som bara finns på papperet. Funktionen Govern inleder ramverket eftersom det här är ledningsbeslut lika mycket som tekniska: någon måste bestämma hur stor risk som är acceptabel, vilken data som är värd mest omsorg och vad resten av skyddet får kosta.

Så ser det ut i praktiken

Säkerhetsarbetet här har tre led: problem fångas när de kommer in, ett system i drift beskrivs ärligt, och det kontrolleras att en åtgärd faktiskt verkar.

Det första är ett kontinuerligt säkerhetsprogram för en applikationsplattform. Statisk analys körs med CodeQL, dynamisk testning med ZAP, och Go-beroenden kontrolleras med govulncheck. En materialförteckning för programvaran genereras vid varje bygge med Anchore och Syft, Gitleaks söker igenom historiken efter inloggningsuppgifter, och arbetsflödena refererar till actions från tredje part med commit-hash, så att den som flyttar en tagg inte kan byta ut koden de kör. Dependabot bevakar 6 ekosystem. Vid sidan av automatiseringen finns 21 skriftliga säkerhetsgranskningar, bland dem en hotmodell och en bedömning mot testguiden från OWASP. En sårbarhet som de konfigurerade kontrollerna känner igen kan få bygget att misslyckas. Sidan säger rakt ut vad det kostar: mängden fynd och den löpande triagering som krävs för att signalen ska förbli användbar.

Det andra är en uppsättning sju skrivskyddade roller som återger värden i drift som Markdown, byggda eftersom en stack för mätvärden inte ryms på värdens 464 MB. Åtkomstrapporten täcker konton, sudo-omfattning, nyckelfingeravtryck, användare i git-forgen och databasroller. Säkerhetsrapporten svarar på om härdningen upprätthålls och inte bara är konfigurerad, och skriver ut brandväggsreglerna i matchningsordning och den aktiva regeluppsättningen för spärrar, och inget tal skrivs ut som körningen inte har mätt. Rapporterna hittade bl.a. två döda säkerhetsåtgärder och en odeklarerad lyssnande nätverksport.

Det tredje visar varför den skillnaden spelar roll. På samma värd i företagets drift låg en hastighetsbegränsning i ett år under en bredare brandväggsregel som matchade först, så inget paket nådde någonsin fram till den. Kontrollerna läser nu den numrerade regellistan och den aktiva filterkedjan och verifierar mot ordningen. Varje port har exakt en regel, alltid med ett protokoll, SSH-porten har en hastighetsbegränsning och aldrig en allow-regel bredvid sig, och den deklarerade publika ytan på fem portar verifieras som helhet.

Var det går fel

En åtgärd är konfigurerad men upprätthålls aldrig. En inställning i en fil, en regel i en lista eller en policy på en wiki dokumenterar vad någon hade för avsikt. Bara en kontroll mot det körande systemet visar vad som är sant. Ett program som räknar åtgärder i stället för att testa dem rapporterar full täckning medan luckorna står öppna, och det första riktiga testet kommer från någon annan.

Allt vilar på ett enda lager. Ett starkt yttre skal med vidöppen åtkomst bakom sig betyder att ett enda misstag lämnar ut allt. Djupförsvar utgår från att varje lager kommer att brista någon gång och placerar ett till bakom det, så att ett stulet lösenord ändå möter en andra faktor och en kompromitterad tjänst ändå möter en snäv databasroll.

Fynden kommer snabbare än någon hinner läsa dem. En skanner som rapporterar varje tänkbart problem som lika brådskande lär folk att sluta läsa. Tydliga ägare, gränsvärden för allvarlighetsgrad och en skriven regel för när ett fynd stoppar en release gör att det skannern skriver ut förblir värt att läsa.

Tillgängligheten kommer man ihåg först under driftstoppet. Konfidentialiteten får mest uppmärksamhet eftersom läckor blir nyheter. Säkerhetskopior som aldrig har återställts, en ensam server utan plan för hur den ska ersättas och certifikat som löper ut obemärkt brister alla i den tredje egenskapen, och de brukar göra det på den sämsta tänkbara dagen.

Rapporter från utomstående hamnar i fel inkorg. Den som hittar en svaghet i en publik tjänst behöver veta var den ska säga till. RFC 9116 definierar filen security.txt, som serveras från /.well-known/security.txt, med ett obligatoriskt fält Contact som anger vart rapporterna ska och ett obligatoriskt fält Expires som anger hur länge filen går att lita på. Annars landar rapporterna i en allmän inkorg eller hos den som svarar först.

Läs mer

- Information security, in the NIST CSRC glossary — definitionen från FIPS 200 och 44 U.S.C. 3552, med dess tre egenskaper.
- 44 U.S.C. 3552 — lagtexten som definierar konfidentialitet, riktighet och tillgänglighet.
- NIST SP 800-53 Rev. 5 — katalogen över säkerhets- och integritetsåtgärder, ordnade i familjer.
- The NIST Cybersecurity Framework 2.0 — sex funktioner som beskriver säkerhetsutfall, från Govern till Recover.
- RFC 9116 — formatet security.txt, som talar om för forskare var en sårbarhet ska rapporteras.

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 informationssäkerhet?” 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/security/