Engineer

Sikkerhet

vern av data og systemer mot misbruk og skade

Hva det er

Sikkerhet, eller informasjonssikkerhet med det fulle navnet, er faget som holder informasjon, og systemene som lagrer og flytter den, i den tilstanden eierne har tenkt: lest bare av dem som skal lese den, endret bare på de måtene som var meningen, og til stede når den trengs. I daglig tale og i de fleste stillingstitler blir det bare sikkerhet. Definisjonen i ordlisten til NIST er hentet fra amerikansk føderal lov, 44 U.S.C. 3552, som nevner tre egenskaper. Konfidensialitet bevarer autoriserte begrensninger på tilgang og utlevering. Integritet verner mot uriktig endring eller ødeleggelse, og omfatter å kunne vise at informasjonen er ekte, og at avsenderen ikke troverdig kan nekte for å ha sendt den. Tilgjengelighet betyr rettidig og pålitelig tilgang til informasjonen og bruk av den.

De tre drar i hver sin retning, og den spenningen er det meste av det som gjør arbeidet vanskelig. En database ingen kan nå, er helt konfidensiell og til ingen nytte. En sikkerhetskopi som ligger tre steder, bedrer tilgjengeligheten og gir en tyv tre steder å lete. De fleste beslutningene i faget handler om hvor man skal plassere seg mellom disse kreftene for én bestemt type informasjon, og svaret for en offentlig prisliste er et helt annet enn svaret for en pasientjournal.

Arbeidet gjøres gjennom tiltak, hvert av dem et bestemt vern med et bestemt formål. Noen er tekniske: kryptering, autentisering, en brannmur, tilgangskontroll. Noen er organisatoriske: en gjennomgang før en endring går ut, en regel om at den som slutter, mister tilgangen den siste arbeidsdagen, en skriftlig plan for en driftshendelse. Noen er fysiske, som et låst rom. NIST SP 800-53 er en katalog over slike kontroller, gruppert i familier og skrevet slik at en organisasjon kan velge dem som passer risikoene sine. NIST Cybersecurity Framework 2.0 virker ett nivå høyere. Det beskriver resultater under seks funksjoner, Govern, Identify, Protect, Detect, Respond og Recover, og sier selv at det ikke foreskriver hvordan resultatene skal oppnås.

Bruk begrepet i en beslutning

Bruk «Hva er sikkerhet?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Kontoer, passord og tilganger ordnet slik at folk har nøyaktig den tilgangen jobben krever, og de som slutter, mister den samme dag.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Skrev 1 000 RBAC-regler for å sikre Linux-servere — 1,000 tilgangsregler skrevet for å tette et sikkerhetshull

Skrev 1 000 RBAC-regler for å sikre Linux-servere Ta kontakt →

Hvorfor det er viktig

Skade på informasjon er vanskelig å rette opp. Data som har lekket, forblir lekket, uansett hva som rettes etterpå. En post som ble endret uten at noen merket det, gjør hver senere beslutning som bygde på den, tvilsom. Et brudd i tilgjengeligheten den dagen lønnskjøringen eller anbudsfristen faller, koster mer enn timene det varer. De som dataene handlet om, bærer som regel kostnaden først, og selskapet som holdt dem, bærer den etterpå.

For en kjøper er det vanskelige at sikkerhet er usynlig så lenge den virker. To leverandører kan liste opp de samme verktøyene med de samme ordene, og bare den ene har kanskje sjekket at verktøyene gjør det listen sier. De nyttige spørsmålene handler derfor om bevis: hvilke tiltak som er på plass, hvordan noen vet at de virker i dag og ikke bare den dagen de ble satt opp, og hva som skjer når ett av dem melder om et problem. En leverandør som svarer med en rapport generert fra det kjørende systemet, står et annet sted enn en som svarer med et policydokument.

Avveiningene er ekte, og de handler mest om tid og friksjon. Hver skanner gir funn, og hvert funn trenger et menneske som avgjør om det betyr noe. Hvert ekstra steg ved innlogging er et steg folk vil lete etter veier rundt. Hvert tiltak som legges til, må vedlikeholdes, ellers blir det i det stille et tiltak som bare finnes på papiret. Govern-funksjonen åpner rammeverket fordi dette er ledelsesbeslutninger like mye som tekniske: noen må avgjøre hvor mye risiko som er akseptabelt, hvilke data som fortjener mest omsorg, og hva resten av vernet skal koste.

Slik ser det ut i praksis

Å fange problemer idet de kommer, å beskrive et kjørende system ærlig og å sjekke at et tiltak faktisk gjelder, er tre deler av det samme faget, og hver av dem har et eget arbeid her.

Det første er et løpende sikkerhetsprogram for en applikasjonsplattform. Statisk analyse kjøres gjennom CodeQL, dynamisk testing gjennom ZAP, og Go-avhengigheter sjekkes med govulncheck. En stykkliste for programvaren lages ved hver bygging med Anchore og Syft, Gitleaks skanner historikken etter påloggingsinformasjon, hver GitHub Action fra tredjepart er låst til en commit-hash, og Dependabot overvåker 6 økosystemer. Ved siden av automatiseringen ligger 21 skriftlige sikkerhetsrevisjoner, bl.a. en trusselmodell og en vurdering opp mot OWASPs testveiledning. En sårbarhet som de konfigurerte sjekkene gjenkjenner, kan få byggingen til å feile. Siden sier rett ut hva det koster: mengden funn, og den løpende triageringen som skal til for at signalet forblir brukbart.

Det andre er sju skrivebeskyttede roller som gjengir verten i drift som Markdown, bygd fordi en stack for metrikker ikke får plass på vertens 464 MB. Tilgangsrapporten dekker kontoer, sudo-omfang, nøkkelfingeravtrykk, forge-brukere og databaseroller. Sikkerhetsrapporten svarer på om herdingen håndheves og ikke bare er konfigurert, ved å skrive ut brannmurreglene i treffrekkefølge og det aktive regelsettet for blokkeringer, og den skriver bare ut tall som kjøringen faktisk har målt. Rapportene fant bl.a. to døde sikkerhetstiltak og en lyttende nettverksport som ikke var deklarert.

Det tredje viser hvorfor den forskjellen betyr noe. På den samme verten hos selskapet lå en hastighetsbegrensning i et år under en bredere brannmurregel som slo til først, så ingen pakke nådde den noen gang. Sjekkene leser nå den nummererte regeloversikten og den aktive filterkjeden, og kontrollerer mot rekkefølgen. Hver port har nøyaktig én regel, alltid med protokoll, SSH-porten har en hastighetsbegrensning og aldri en allow-regel ved siden av, og den deklarerte offentlige flaten på fem porter kontrolleres som en helhet.

Hvor det går galt

Et tiltak som er konfigurert, men aldri håndhevet. En innstilling i en fil, en regel i en liste eller en policy på en wiki viser hva noen hadde tenkt. Bare en sjekk mot det kjørende systemet viser hva som er sant. Et program som teller tiltak i stedet

for å teste dem, rapporterer full dekning mens hullene står åpne, og den første virkelige testen kommer fra noen andre.

Alt hviler på ett lag. En sterk ytre grense med vid tilgang bak seg betyr at én enkelt feil gir bort alt. Lagdelt forsvar, defence in depth, går ut fra at hvert lag vil svikte en gang og legger et nytt bak det, slik at et stjålet passord fortsatt møter en ekstra faktor, og en kompromittert tjeneste fortsatt møter en smal databaserolle.

Funn som kommer raskere enn noen leser dem. En skanner som melder hvert mulige problem med samme hastegrad, lærer folk å slutte å lese den. Tydelige eiere, terskler for alvorlighetsgrad og en skriftlig regel for når et funn stopper en utgivelse, bidrar til at resultatet fortsatt er verdt å lese.

Tilgjengelighet som huskes først under nedetiden. Konfidensialitet får mest oppmerksomhet, fordi lekkasjer kommer i nyhetene. Sikkerhetskopier som aldri er gjenopprettet, én enkelt server uten plan for erstatning og sertifikater som utløper uten at noen merker det, svikter alle på den tredje egenskapen, og de pleier å svikte på den verst tenkelige dagen.

Utenforstående som leter etter et sted å melde fra. Den som finner en svakhet i en offentlig tjeneste, trenger å vite hvor det skal sies fra. RFC 9116 definerer en security.txt-fil, servert fra /.well-known/security.txt, med et påkrevd Contact-felt som sier hvor rapporter skal sendes, og et påkrevd Expires-felt som sier hvor lenge filen kan stoles på. Rapportene havner ellers i en generell innboks eller hos den som svarer først.

Les mer

- Information security, in the NIST CSRC glossary — definisjonen fra FIPS 200 og 44 U.S.C. 3552, med de tre egenskapene.
- 44 U.S.C. 3552 — lovteksten som definerer konfidensialitet, integritet og tilgjengelighet.
- NIST SP 800-53 Rev. 5 — katalogen over sikkerhets- og personvernkontroller, gruppert i familier.
- The NIST Cybersecurity Framework 2.0 — seks funksjoner som beskriver sikkerhetsresultater, fra Govern til Recover.
- RFC 9116 — security.txt-formatet som forteller forskere hvor de kan melde en sårbarhet.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er sikkerhet?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/security/