Engineer

It-sikkerhed

beskyttelse af data og systemer mod misbrug og skade

Hvad det er

It-sikkerhed er arbejdet med at holde information og de systemer, der gemmer og flytter den, i den tilstand, ejerne har tænkt sig: læst kun af dem, der skal læse den, ændret kun på de måder, det var meningen, og til stede, når der er brug for den. I daglig tale og i de fleste jobtitler hedder det bare sikkerhed, og når man taler om sikkerheden i et bestemt system, mener man som regel det samme. Definitionen i NIST's ordliste kommer fra amerikansk føderal lov, 44 U.S.C. 3552, som nævner tre egenskaber. Fortrolighed bevarer de tilladte begrænsninger på adgang og videregivelse. Integritet beskytter mod ukorrekt ændring eller sletning og omfatter, at man kan vise, at informationen er ægte, og at afsenderen ikke troværdigt kan benægte at have sendt den. Tilgængelighed betyder rettidig og pålidelig adgang til informationen og brugen af den.

De tre trækker i hver sin retning, og det er netop den spænding, der gør arbejdet svært. En database, som ingen kan nå, er fuldstændig fortrolig og til ingen nytte. En backup, der ligger tre steder, forbedrer tilgængeligheden og giver en tyv tre steder at lede. De fleste beslutninger på området handler om, hvor man skal placere sig mellem de tre for én bestemt slags information, og svaret for en offentlig prisliste er et helt andet end svaret for en patients journal.

Arbejdet sker gennem kontroller, hver af dem en bestemt beskyttelse med et bestemt formål. Nogle er tekniske: kryptering, autentificering, en firewall, adgangskontrol. Nogle er procedurer: en gennemgang, før en ændring sendes ud, en regel om, at medarbejdere, der stopper, mister adgang på deres sidste dag, en skriftlig plan for en hændelse. Nogle er fysiske, som et aflåst rum. NIST SP 800-53 er et katalog over den slags kontroller, ordnet i familier og skrevet, så en organisation kan vælge dem, der passer til dens risici. NIST Cybersecurity Framework 2.0 arbejder et niveau højere oppe. Den beskriver resultater under seks funktioner, Govern, Identify, Protect, Detect, Respond og Recover, og siger udtrykkeligt, at den ikke foreskriver, hvordan resultaterne skal nås.

Brug begrebet i en beslutning

Brug »Hvad er it-sikkerhed?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Konti, adgangskoder og rettigheder sat op, så folk har præcis den adgang, jobbet kræver, og fratrådte mister den samme dag.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har skrevet 1.000 RBAC-regler til Linux-servere — 1,000 adgangsregler skrevet for at lukke et sikkerhedshul

Har skrevet 1.000 RBAC-regler til Linux-servere Kontakt os →

Hvorfor det betyder noget

Skade på information er svær at rette op på. Data, der er lækket, forbliver lækket, uanset hvad der bliver rettet bagefter. En registrering, der blev ændret, uden at nogen opdagede det, gør alle senere beslutninger, der byggede på den, tvivlsomme. Et nedbrud på den dag, hvor lønkørslen eller en tilbudsfrist falder, koster mere end de timer, det varer. Det er som regel dem, hvis data det var, der betaler først, og virksomheden, der havde dem, bagefter.

For en køber er det svære, at sikkerhed er usynlig, så længe den virker. To leverandører kan opremse de samme værktøjer med de samme ord, og måske har kun den ene af dem tjekket, at værktøjerne gør det, listen siger. De nyttige spørgsmål handler derfor om dokumentation: hvilke kontroller er på plads, hvordan ved nogen, at de virker i dag og ikke kun den dag, de blev installeret, og hvad sker der, når en af dem melder et problem? En leverandør, der svarer med en rapport genereret fra det kørende system, står et andet sted end en, der svarer med et politikdokument.

Afvejningerne er reelle og handler mest om tid og gnidninger. Hver scanner giver fund, og hvert fund kræver et menneske, der afgør, om det betyder noget. Hvert ekstra trin ved login er et trin, folk vil lede efter veje uden om. Hver kontrol, der bliver tilføjet, skal vedligeholdes, ellers bliver den i det stille en kontrol, der kun findes på papir. Govern-funktionen står først i rammeværket, fordi det her er ledelsesbeslutninger lige så meget som tekniske: nogen skal afgøre, hvor meget risiko der er acceptabel, hvilke data der fortjener mest omhu, og hvad resten af beskyttelsen må koste.

Sådan ser det ud i praksis

Problemer skal fanges, når de opstår, og det er opgaven for et løbende sikkerhedsprogram for en applikationsplatform. Statisk analyse kører gennem CodeQL, dynamisk test gennem ZAP, og Go-afhængigheder tjekkes med govulncheck. En SBOM genereres ved hvert build med Anchore og Syft, Gitleaks gennemsøger historikken efter adgangsoplysninger, hver GitHub Action fra en tredjepart er låst til en commit-hash, og Dependabot holder øje med 6 økosystemer. Ved siden af automatiseringen ligger 21 skriftlige sikkerhedsgennemgange, heriblandt en trusselsmodel og en vurdering op mod OWASP-testguiden. En sårbarhed, som de konfigurerede tjek genkender, kan få buildet til at fejle. Siden nævner prisen ligeud: mængden af fund og den løbende triage, der skal til for at holde signalet brugbart.

At beskrive et kørende system ærligt er opgaven for syv skrivebeskyttede roller, der gengiver en kørende vært som Markdown, bygget fordi en metrikstak ikke kan være på værtens 464 MB. Adgangsrapporten dækker konti, sudo-omfang, nøglefingeraftryk, forge-brugere og databaseroller. Sikkerhedsrapporten besvarer, om hærdningen er håndhævet og ikke blot konfigureret, og udskriver firewallreglerne i den rækkefølge, de matches i, og det aktive regelsæt for blokeringer. Der udskrives intet tal, som kørslen ikke har målt. Blandt andet fandt rapporterne to døde sikkerhedskontroller og en ikke-erklæret lyttende port.

Hvorfor det betyder noget at tjekke, at en kontrol faktisk virker, viste sig på den samme vært: en hastighedsbegrænsning lå i et år under en bredere firewallregel, der matchede først, så ingen pakke nogensinde nåede den. Tjekkene læser nu den nummererede regeloversigt og den aktive filterkæde og efterprøver rækkefølgen. Hver port har præcis én regel, altid med en protokol, SSH-porten har en hastighedsbegrænsning og aldrig en tilladelse ved siden af, og den erklærede offentlige overflade på fem porte efterprøves som en helhed.

Hvor det går galt

En kontrol er konfigureret og bliver aldrig håndhævet. En indstilling i en fil, en regel i en liste eller en politik på en wiki fortæller, hvad nogen havde tænkt sig. Kun et tjek mod det kørende system viser, hvad der er sandt. Et program, der tæller kontroller i stedet for at teste dem, rapporterer fuld dækning, mens hullerne står åbne, og den første rigtige test kommer udefra.

Alt hviler på ét lag. En stærk ydre grænse med vid åben adgang bag sig betyder, at en enkelt fejl giver alt væk. Lagdelt forsvar regner med, at hvert lag svigter på et tidspunkt, og stiller et nyt bag det, så en stjålet adgangskode stadig møder en anden faktor, og en kompromitteret tjeneste stadig møder en snæver databaserolle.

Fundene kommer hurtigere, end nogen læser dem. En scanner, der melder alle tænkelige problemer som lige presserende, lærer folk at holde op med at læse den. Klare ejere, grænser for alvorlighed og en skriftlig regel for, hvornår et fund stopper en udgivelse, gør resultatet værd at læse.

Tilgængelighed huskes først under nedbruddet. Fortrolighed får mest opmærksomhed, fordi læk kommer i nyhederne. Backups, der aldrig er blevet gendannet, en enkelt server uden plan for, hvad der skal erstatte den, og certifikater, der udløber ubemærket, svigter alle den tredje egenskab, og de gør det helst på den værst tænkelige dag.

Udefrakommende har ikke noget oplagt sted at melde et problem. Den, der finder en svaghed i en offentlig tjeneste, skal vide, hvor det skal meldes. RFC 9116 definerer en security.txt-fil, der serveres fra /.well-known/security.txt, med et påkrævet Contact-felt, der siger, hvor meldinger skal sendes hen, og et påkrævet Expires-felt, der siger, hvor længe filen kan stoles på. Uden den lander meldingerne i en fælles indbakke eller hos den, der tilfældigvis svarer først.

Læs mere

- Information security i NIST CSRC's ordliste — definitionen fra FIPS 200 og 44 U.S.C. 3552 med de tre egenskaber.
- 44 U.S.C. 3552 — loven, der definerer fortrolighed, integritet og tilgængelighed.
- NIST SP 800-53 Rev. 5 — kataloget over sikkerheds- og privatlivskontroller, ordnet i familier.
- NIST Cybersecurity Framework 2.0 — seks funktioner, der beskriver sikkerhedsresultater fra Govern til Recover.
- RFC 9116 — formatet security.txt, der fortæller forskere, hvor en sårbarhed skal meldes.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er it-sikkerhed?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/security/