Engineer

Adgangskontrol

at give eller nægte hver anmodning om en ressource

Hvad det er

Adgangskontrol er den del af et system, der besvarer ét spørgsmål mange gange i sekundet: må den, der spørger, gøre det her ved den her ressource lige nu? Den, der spørger, kan være en person, en tjeneste eller et planlagt job. Ressourcen kan være en fil, en række i en database, et API-endepunkt, et git-repository eller en dør. Når man taler om den konkrete mekanisme i et bestemt system, siger man ofte adgangskontrollen, og NIST's ordliste nævner autorisation som et synonym for hele idéen. Definitionerne dér dækker begge halvdele af arbejdet: beslutningen om at tillade eller nægte et subjekt adgang til objekter i systemet, og processen med at imødekomme eller afvise bestemte anmodninger om at hente og bruge information og de tjenester, der behandler den, eller om at komme ind i bestemte fysiske lokaler.

Den er let at blande sammen med autentificering, men det er to forskellige trin. NIST SP 800-162 siger det ligeud: autentificering er ikke det samme som adgangskontrol. Autentificering fastslår, hvem der spørger. Adgangskontrol tager den identitet, sammen med det, man ellers ved om anmodningen, og afgør, hvad den, der spørger, må. Et system kan verificere en person fejlfrit og alligevel lade vedkommende læse poster, der tilhører en anden, fordi det andet spørgsmål aldrig blev stillet.

Samme vejledning deler arbejdet i to. Et beslutningspunkt beregner svaret, og et håndhævelsespunkt sidder i anmodningens vej og fører svaret ud i livet. De kan godt bo i samme proces, men det er værd at holde dem adskilt i tankerne, for en beslutning, som intet håndhæver, beskytter ingenting. NIST SP 800-53 skriver det ind i to kontroller: AC-24 beder om, at beslutningerne anvendes på hver anmodning før håndhævelsen, og AC-3 beder om, at godkendte autorisationer bliver håndhævet.

Reglerne kan have flere former: en liste over tilladte identiteter på hvert objekt, roller som i RBAC eller attributter ved den, der spørger, ved objektet, handlingen og omgivelserne, som er emnet for SP 800-162. Uanset formen skal noget stadig stille spørgsmålet ved hver eneste anmodning.

Brug begrebet i en beslutning

Brug »Hvad er adgangskontrol?« 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

Når nogen er logget ind, er næsten alt, vedkommende kan nå, bestemt af adgangskontrollen. Stærk autentificering foran svag adgangskontrol registrerer blot, hvilken konto der tog dataene. For en virksomhed, der passer på andres oplysninger, er det her, et løfte om, hvem der ser hvad, holder eller brister.

NIST beskriver den ideelle håndhævelse som en referencemonitor. Kontrol AC-25 i SP 800-53 beder om en, der ikke kan manipuleres, altid bliver kaldt og er lille nok til at kunne analyseres og testes. De tre egenskaber fungerer som en praktisk prøve på ethvert tjek i et rigtigt produkt. Kan den, der spørger, ændre de input, tjekket bygger på, dumper det på den første. Findes der en vej til dataene, der ikke går gennem tjekket, dumper det på den anden. Er logikken spredt over hundredvis af handlere, så ingen kan læse den fra ende til anden, dumper det på den tredje.

OWASP Application Security Verification Standard gør det til krav, et team kan teste imod. Kapitlet om autorisation beder om, at adgang til funktioner begrænses til dem med en udtrykkelig tilladelse, at adgang til bestemte dataposter begrænses på samme måde, og at reglerne håndhæves i et betroet servicelag i stedet for at hvile på noget, en ikke-betroet klient kan manipulere, som JavaScript i browseren. Den beder også om, at en ændring af de værdier, en beslutning bygger på, træder i kraft med det samme, og at en afbødende kontrol slår alarm, hvis nogen handler efter at have mistet retten, når ændringen ikke kan træde i kraft med det samme.

Afvejningen er en pris på anmodningens vej. Hver beslutning kræver fakta, og hvert faktum kræver et opslag. Springer man opslaget over, ender tjekket som regel der, hvor det er billigst, og det er ofte det sted, den, der spørger, selv styrer.

Sådan ser det ud i praksis

En bruger på en maritim platform kan handle på vegne af flere organisationer. Den aktive organisation ligger på klienten, og ingen adgangsbeslutning bygger på den. En OrganizationContext gemmer det aktuelle valg i localStorage, så skiftet sker øjeblikkeligt, og en cookie på serversiden spejler det, så serverrenderede sider når frem til den samme kontekst. Autorisationen kontrolleres igen på serveren ved hver anmodning. Siden trækker grænsen i én sætning: serveren er den eneste instans, der afgør, hvad brugeren må, og den, der piller ved localStorage, ændrer kun, hvad vedkommendes egen brugerflade viser, for serveren siger stadig nej.

På den samme slags platform blev det at tage imod penge og det at give adgang bygget som to systemer. Kort gennem Stripe og køb i apps fra Apple og Google løber sammen i et payments-skema på 9 tabeller og 34 funktioner. Et separat access-skema på 11 tabeller og 34 funktioner svarer på »må denne konto det her?« uden at vide, hvilken butik der betalte. Det svar styrer adgangen til virksomhedskataloget, søgningen og dataeksporten, og det kontrolleres igen på serveren ved hver anmodning, for en skjult knap er en høflighed og ikke en kontrol. En ny butik rører nu kun ved payments-siden, og et supportspørgsmål om nogens adgang har én tabel at kigge i frem for tre. Siden nævner prisen: to skemaer og et rettighedsopslag på anmodninger, der ellers ville have været gratis.

Da virksomheden flyttede sin kildekode over på egen hardware, blev git-forgen sat op til at afvise som standard. Siden regner adgangskontrol blandt det, man påtager sig ved at køre en forge selv. Forgen blev valgt, fordi den ikke har nogen administrativ webgrænseflade, ud fra tanken om, at jo mindre grænseflade, jo mindre at forsvare. Reglerne er få og strenge: en forbindelse, der ikke siger, hvem den er, kommer ikke ind, det gør en uden nøgle heller ikke, og hvert erklæret repository står som privat frem for at være gemt af vejen i håb om, at ingen finder det. Selv lytteren hører med til adgangskontrollen. SSH-porten, 23231, svarer kun på loopback, så vejen dertil går over en jump host, og en multiplexer, der ville åbne git over den offentlige port, er skrevet og slået fra, fordi en lytter, som ingen bruger, er angrebsflade.

Hvor det går galt

Tjekket bor i brugerfladen. En knap er skjult eller gjort grå, og endepunktet bag den svarer alle, der kalder det direkte. Serveren skal træffe beslutningen igen ved hver anmodning, ud fra fakta, som den, der spørger, ikke kan redigere.

Funktionen bliver tjekket, posten bliver ikke. En anmodning udpeger en faktura, et dokument eller en konto med dens id, serveren bekræfter, at den, der spørger, må se fakturaer, og sender den efterspurgte tilbage uden at tjekke, hvem den tilhører. ASVS kalder hullet insecure direct object reference (IDOR) eller broken object level authorization (BOLA). En forsvarer genkender det på et id i en anmodning, som serveren bruger, som det er. Løsningen er at slå hvert objekt op inden for den spørgendes eget område, og i et produkt med flere kunder at tage kunden fra sessionen på serveren og aldrig fra anmodningen.

Alt nyt står åbent, til nogen lukker det. En ny rute, en ny tabel eller et nyt repository starter med det, standarden end er, og er standarden at tillade, findes hullet, indtil nogen opdager det. SP 800-53 formulerer den modsatte regel for netværkstrafik som afvis som standard, tillad som undtagelse, og den samme regel passer på alle lag: det, der aldrig er givet, afvises.

Tildelinger vokser kun. SP 800-162 bemærker, at når adgang ikke fjernes eller tilbagekaldes over tid, samler brugerne privilegier op. Folk skifter team, projekter slutter, og konsulenter tager videre, og hver af de begivenheder er et tidspunkt, hvor noget burde fjernes. En tilbagekaldelse, der først virker, når en session udløber timer senere, er en blødere udgave af det samme hul.

Ingen kan sige, hvorfor en anmodning blev tilladt. Når beslutninger træffes mange steder og logges intetsteds, har en undersøgelse intet at læse. Log tildelinger og afvisninger sammen med den regel, der gav dem, og beskyt den log: SP 800-162 advarer om, at mønsteret i beslutningerne kan afsløre attributter ved de mennesker, der står bag anmodningerne.

Læs mere

- Access control i NIST CSRC's ordliste — definitioner fra FIPS 201-3 og CNSSI 4009, med autorisation nævnt som synonym.
- NIST SP 800-53 Rev. 5 — familien for adgangskontrol, herunder AC-3 om håndhævelse, AC-24 om beslutninger og AC-25.

- NIST SP 800-162 — attributbaseret adgangskontrol med beslutnings- og håndhævelsespunkter.
- OWASP Application Security Verification Standard — testbare krav til autorisation på niveau med funktioner, data og felter.

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 adgangskontrol?« 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/access-control/