Engineer

Tilgangskontroll

å gi eller nekte hver forespørsel om å bruke en ressurs

Hva det er

Tilgangskontroll er den delen av et system som svarer på ett og samme spørsmål mange ganger i sekundet: får den som spør, gjøre akkurat dette med akkurat denne ressursen, akkurat nå? Den som spør, kan være en person, en tjeneste eller en planlagt jobb. Ressursen kan være en fil, en rad i en database, et API-endepunkt, et git-repo eller en dør. Når det er snakk om mekanismen i ett bestemt system, sier man gjerne tilgangskontrollen. NIST-ordlisten oppgir autorisasjon som synonym for hele idéen, og definisjonene der dekker begge halvdelene av jobben: beslutningen om å tillate eller avslå at et subjekt når objekter i systemet, og prosessen som innvilger eller avviser konkrete forespørsler om å hente og bruke informasjon og tilhørende tjenester, eller om å komme inn i bestemte fysiske lokaler.

Tilgangskontroll blandes lett sammen med autentisering, men det er to atskilte trinn. NIST SP 800-162 sier det rett ut: autentisering er ikke det samme som tilgangskontroll. Autentisering fastslår hvem som spør. Tilgangskontrollen tar den identiteten, sammen med alt annet som er kjent om forespørselen, og avgjør hva den som spør, får gjøre. Et system kan verifisere en person feilfritt og likevel la vedkommende lese poster som tilhører noen andre, fordi det andre spørsmålet aldri ble stilt.

Den samme veiledningen deler arbeidet i to. Et beslutningspunkt (policy decision point) regner ut svaret, og et håndhevingspunkt (policy enforcement point) står i veien for forespørselen og setter svaret ut i livet. Begge kan bo i én og samme prosess, men skillet er verdt å ha i hodet, for en beslutning som ingenting håndhever, beskytter ingenting. NIST SP 800-53 skriver dette inn i to kontroller: AC-24 krever at beslutningene anvendes på hver tilgangsforespørsel før håndhevingen, og AC-3 krever at godkjente autorisasjoner faktisk håndheves.

Reglene kan ha flere former: en liste over tillatte identiteter på hvert objekt, roller som i RBAC, eller attributter ved den som spør, ved objektet, ved handlingen og ved omgivelsene, som er temaet for SP 800-162. Uansett form må noe fortsatt stille spørsmålet ved hver eneste forespørsel.

Bruk begrepet i en beslutning

Bruk «Hva er tilgangskontroll?» 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

Når noen først er logget inn, er nesten alt vedkommende kan nå, bestemt av tilgangskontrollen. Sterk autentisering foran svak tilgangskontroll registrerer bare hvilken konto som tok dataene. For en virksomhet som forvalter andres opplysninger, er det her et løfte om hvem som ser hva, holder eller brister.

NIST beskriver den ideelle håndhevingsmekanismen som en referansemonitor (reference monitor). Kontroll AC-25 i SP 800-53 ber om en som ikke kan manipuleres, som alltid blir kalt, og som er liten nok til å analyseres og testes. De tre egenskapene fungerer som en praktisk prøve på enhver sjekk i et ekte produkt:

- Kan den som spør, endre inndataene sjekken bygger på, stryker den på den første.
- Finnes det en vei til dataene som går utenom sjekken, stryker den på den andre.
- Er logikken spredt over hundrevis av handlere, slik at ingen kan lese den fra ende til annen, stryker den på den tredje.

OWASP Application Security Verification Standard (ASVS) gjør dette om til krav et team kan teste mot. Kapittelet om autorisasjon krever at tilgang til funksjoner begrenses til dem som har uttrykkelig tillatelse, at tilgang til bestemte dataelementer begrenses på samme måte, og at reglene håndheves i et betrodd tjenestelag i stedet for å hvile på noe en ikke-betrodd klient kan manipulere, slik som JavaScript som kjører i nettleseren. Standarden krever også at en endring i

verdiene en beslutning bygger på, får virkning med en gang. Må endringen vente, skal et kompenserende tiltak slå alarm når noen handler etter å ha mistet retten til det.

Avveiningen er en kostnad på forespørselens vei. Hver beslutning trenger fakta, og hvert faktum trenger et oppslag. Hopper man over oppslaget, havner sjekken gjerne der den er billigst, og det er ofte nettopp det stedet den som spør, selv styrer.

Slik ser det ut i praksis

Tre oppdrag på dette nettstedet viser hvor beslutningen tas, og hvem som har lov til å ta den.

På en maritim plattform der én person kan handle på vegne av flere organisasjoner, ligger den aktive organisasjonen på klienten, og ingen tilgangsbeslutning bygger på den. En OrganizationContext lagrer gjeldende valg i localStorage, så byttet skjer umiddelbart, og en cookie på serversiden speiler det, slik at serverrenderte sider får samme kontekst. Autorisasjonen kontrolleres på nytt på serveren ved hver forespørsel. Siden trekker grensen i én setning: serveren er den eneste autoriteten på hva man har lov til å gjøre, og den som tukler med localStorage, endrer bare hva vedkommendes eget brukergrensesnitt viser, for serveren sier fortsatt nei.

På samme type plattform ble det å ta imot penger og det å gi tilgang bygget som to systemer. Kort gjennom Stripe og kjøp i appen via Apple og Google møtes i et databaseskjema for betalinger med 9 tabeller og 34 funksjoner. Et eget skjema for tilgang, med 11 tabeller og 34 funksjoner, svarer på «har denne kontoen lov til å gjøre dette?» uten å vite hvilken salgskanal som betalte. Det svaret styrer tilgangen til bedriftskatalogen, søket og dataeksporten, og serveren henter det fram igjen for hver forespørsel, fordi en skjult knapp er en høflighet og ikke en kontroll. En ny salgskanal berører nå bare betalingssiden, og et brukerstøttespørsmål om noens tilgang har én tabell å se i i stedet for tre. Siden nevner prisen: to skjemaer, og et rettighetsoppslag på forespørsler som ellers ville vært gratis.

Da selskapet flyttet kildekoden sin over på egen maskinvare, ble git-forgen satt opp til å avvise som standard. Siden regner tilgangskontroll blant det man påtar seg når man drifter en forge selv. Forgen ble valgt fordi den er bygd uten administrativt webgrensesnitt, etter tanken om at jo mindre grensesnitt, desto

mindre å forsvare. Hver forespørsel møter et avslag som standard: forgen avviser den som er anonym og den som mangler nøkkel, og hvert deklarert repo er merket som privat i stedet for å stole på at ingen finner det. Lytteren for SSH tar bare imot tilkoblinger på loopback-grensesnittet, port 23231, og utenfra kommer man dit via en jump host. En protokollmultiplekser som ville åpnet git over den offentlige porten, er skrevet og slått av, fordi en lytter som ingen bruker, er angrepsflate.

Hvor det går galt

Sjekken bor i grensesnittet. En knapp skjules eller gråes ut, og endepunktet bak den svarer alle som kaller det direkte. Serveren må ta beslutningen på nytt ved hver forespørsel, ut fra fakta som den som spør, ikke kan redigere.

Funksjonen sjekkes, men posten slipper unna. En forespørsel peker ut en faktura, et dokument eller en konto med identifikatoren sin. Serveren bekrefter at den som spør, får se fakturaer, og sender tilbake den som ble bedt om, uten å sjekke hvem den tilhører. ASVS kaller hullet insecure direct object reference (IDOR) eller broken object level authorization (BOLA). Den som forsvarer et system, kjenner det igjen på en identifikator i forespørselen som serveren bruker slik den kom. Løsningen er å slå opp hvert objekt innenfor den spørrendes eget område, og i et produkt med flere kunder å hente kunden fra sesjonen på serveren, aldri fra forespørselen.

Alt nytt står åpent til noen lukker det. En ny rute, en ny tabell eller et nytt repo starter livet med det som er standard, og er standarden å tillate, finnes hullet til noen oppdager det. SP 800-53 formulerer nettverksvarianten av den motsatte regelen som «nekt som standard, tillat ved unntak», og den samme regelen passer på hvert lag: det som aldri ble gitt, blir avvist.

Tildelinger bare vokser. SP 800-162 påpeker at når tilgang ikke fjernes eller trekkes tilbake over tid, samler brukerne opp privilegier. Folk bytter team, prosjekter avsluttes og innleide konsulenter går videre, og hver gang burde noe vært tatt bort. En tilbaketrekking som først virker når en sesjon utløper timer senere, er en mildere utgave av det samme hullet.

Hvorfor ble forespørselen tillatt? Når beslutninger tas mange steder og logges ingen steder, har en granskning ingenting å lese. Logg tildelinger og avslag sammen med regelen som ga dem, og beskytt den loggen: SP 800-162 advarer

om at mønsteret i beslutningene kan avsløre attributter ved menneskene bak forespørslene.

Les mer

- Access control i NIST CSRC-ordlisten — definisjoner fra FIPS 201-3 og CNSSI 4009, med autorisasjon oppført som synonym.
- NIST SP 800-53 Rev. 5 — kontrollfamilien for tilgangskontroll, bl.a. AC-3 om håndheving, AC-24 om beslutninger og AC-25.
- NIST SP 800-162 — attributtbasert tilgangskontroll med beslutningspunkter og håndhevingspunkter.
- OWASP Application Security Verification Standard — testbare autorisasjonskrav for funksjoner, dataelementer og enkeltfelt.

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 tilgangskontroll?» 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/access-control/