Engineer

IT-bruker

en person eller prosess på personens vegne med systemtilgang

Hva det er

En IT-bruker, i dagligtale bare en bruker og på engelsk *user*, er den eller det som et system utfører arbeid for. I teknisk tekst gjør ordet tre forskjellige jobber, og det meste av forvirringen rundt brukere oppstår når de tre glir over i hverandre.

Den første betydningen er personen: et menneske som åpner et produkt og prøver å få noe gjort. Designere, kundestøtte og produktledere mener som regel denne, og den har ingen fast form inne i systemet. Den andre er kontoen: posten systemet tar vare på for å kjenne igjen noen neste gang, gjerne et navn å logge inn med, en intern identifikator, et sett tillatelser og en status som aktiv eller suspendert. Det meste av applikasjonskoden mener denne. Den tredje er brukeren i operativsystemet: på Unix-lignende systemer en oppføring i brukerdatabasen med et brukernavn og en numerisk bruker-ID. Prosesser som kjører, har bruker-ID-legitimasjon som kjernen bruker til å sjekke tillatelser.

De tre passer sjelden sammen én til én. En person kan ha kontoer i mange tjenester, og retningslinjene for digital identitet fra NIST sier rett ut at én person kan ha flere digitale identiteter, hver av dem unik bare innenfor sin egen tjeneste. Én konto kan deles av flere personer, og det er nesten alltid en feil. Svært mange brukere har dessuten ingen person bak seg i det hele tatt: webserveren, databasen, jobben som tar sikkerhetskopier, og skriptet som ruller ut kode, kjører hver som sin egen bruker i operativsystemet, og har ofte kontoer i andre systemer i tillegg. Derfor lyder definisjonen hos NIST «individual, or (system) process acting on behalf of an individual», altså et menneske eller en prosess som handler på vegne av et menneske.

På en Unix-vert er skillet mellom navn og nummer lett å se:

```
$ id ana
uid=1001(ana) gid=1001(ana) groups=1001(ana)
```

Kjernen arbeider med tallet. POSIX definerer en brukerdatabase som for hver bruker holder brukernavnet, den numeriske bruker-ID-en, en innledende gruppe-ID, en innledende arbeidskatalog og et innledende program som skal startes. Eierskap til filer lagres som tallet, og navnet slås opp først når noe skal vises for et menneske. En prosess bærer dessuten mer enn én bruker-ID: en reell, som sier hvem som startet den, og en effektiv, som sier hvem sine privilegier den bruker akkurat nå.

Applikasjonskontoer gjør som regel det samme skillet. SCIM, standarden som brukes til å klargjøre brukere fra ett system inn i et annet, krever et `userName` som folk ser og logger inn med, unikt i tjenesten og sammenlignet uten hensyn til store og små bokstaver. Ved siden av står en egen `id` som tjenesten tildeler, som holder seg stabil og aldri deles ut på nytt. Et `active` -flagg skiller en suspendert konto fra en som virker.

Bruk begrepet i en beslutning

Bruk «Hva er en IT-bruker?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Den bærbare PC-en, skriveren, påloggingen og e-postkassen, ordnet raskt og på klart og enkelt språk, uten at noen føler seg dum.

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. Etablerte en avdeling for teknisk støtte — 10,000 kunder betjent av en supportavdeling bygd opp fra bunnen av

Etablerte en avdeling for teknisk støtte Ta kontakt →

Hvorfor det er viktig

Hver beslutning om tilgang er en beslutning om en bruker, så et uklart bilde av hvem brukeren er, gir en uklar beslutning. Spørsmålet «får denne personen se denne fakturaen?» besvares i koden som «har denne kontoen, i denne konteksten, en tillatelse som dekker denne posten?», og hvert ledd i den oversettelsen er et sted der den tiltenkte personen og den faktiske kontoen kan gli fra hverandre.

Grensen mellom person og konto er også der ansvaret ligger. Loggene fører opp kontoer. Når hver konto tilhører nøyaktig én person, sier en logglinje hvem som gjorde noe. Når en konto deles, sier loggen hvilken hemmelighet som ble brukt,

men ingenting om hvem som skrev den inn, og å stenge tilgangen for én person betyr å endre den for alle.

Brukere i operativsystemet er et veletablert verktøy for minste privilegium. En tjeneste som kjører som sin egen uprivilegerte bruker, er begrenset av den brukerens tillatelser, ikke bare av fileierskap. Den kan fortsatt endre delte ressurser med skrivetilgang, sende nettverksforespørsler og bruke legitimasjon den har tilgang til. Separate tjenestebrukere reduserer skaden ved en kompromittering; de gir ikke fullstendig isolasjon. Den samme tjenesten kjørt som superbrukeren kan sette hele maskinen i fare. Å gi hvert program en egen bruker er en liten konfigurasjonsendring som snevrer inn tillatelsene som er tilgjengelige når noe går galt.

Til slutt har personer og kontoer ulik levetid. Folk bytter navn, e-postadresse og arbeidsgiver; kontoer suspenderes, slås sammen og slettes. Et system som behandler en egenskap som kan endres, f.eks. en e-postadresse, som identiteten til en konto, vil en dag knytte historikken til én person til en annen.

Slik ser det ut i praksis

På en maritim plattform administrerer fagpersoner organisasjoner, som selskaper og akademier, som ikke har egne påloginger. Siden sier regelen rett ut: personen er kontoen, og organisasjonen er noe vedkommende handler på vegne av. Arbeidet var et kontekstbytte som lar en bruker opptre som enhver organisasjon vedkommende administrerer. localStorage i nettleseren holder på hvilken organisasjon som er aktiv, så byttet skjer umiddelbart, og en informasjonskapsel på serversiden speiler den, slik at serverrenderte sider viser den samme konteksten. Tilgangen avgjøres likevel av ingen av delene. Autorisasjonen sjekkes på nytt på serveren ved hver forespørsel, så den som redigerer den lagrede verdien, endrer bare hva vedkommendes egen skjerm viser.

På selskapets egen vert sendes utgivelser ut av en bruker i operativsystemet med nesten ingen rettigheter. Da containerlaget ble satt opp, ble produksjonssetting skilt fra provisjonering. Root setter opp stien for produksjonssetting én gang. Etter det er utgivelsen jobben til en vanlig konto uten privilegier, som bare har lov til å kjøre ett fast skript, og regelen som gir den lov, godtar den ene kommandoen uten argumenter. En rutinemessig utgivelse bygger imaget og starter tjenesten på nytt, og det skjer uten at noen åpner et root-skall.

Å vite hvem brukerne er, er i seg selv en rapport. En av sju skrivebeskyttede rapporteringsroller gjengir en tilgangsrapport fra den levende verten som Markdown i repoet, med kontoer, sudo-omfang, nøkkelfingeravtrykk, brukerne av git-forgen og databaseroller side om side. Regelen for alle sju rapportene er at det ikke skrives ut noe tall som kjøringen ikke har målt. Til sammen har rapportene funnet virkelige ting, bl.a. to døde sikkerhetstiltak og en lyttende port som aldri var deklarert.

Hvor det går galt

En slettet bruker kommer tilbake som en annen. En konto fjernes, identifikatoren deles senere ut igjen, og nykommeren arver alt som fortsatt peker på den gamle verdien: rader i en tabell, en plass på en liste, filer på disk. På en Unix-vert beholder filene en fjernet bruker eide, sin numeriske eier, og den neste brukeren som opprettes med det tallet, eier dem. Gi kontoer identifikatorer som aldri brukes om igjen, slik SCIM krever av sin `id`, og bestem hva som skal skje med dataene til en bruker som slutter, før brukeren fjernes.

En e-postadresse brukes som konto. Den ser ut som en naturlig nøkkel helt til noen bytter adresse, mister tilgangen til en gammel, eller en arbeidsgiver gir en adresse videre til en ny ansatt. Da blir historikken til én person knyttet til en annen, eller én person ender opp med to kontoer. Behold en stabil intern identifikator som nøkkel, og behandle adressen som en egenskap som kan endres.

Alle logger inn med den samme kontoen. En delt administratorinnlogging er rask å sette opp og umulig å revidere. Når noen slutter, tar tilgangen deres slutt bare hvis hemmeligheten endres for alle, og loggen navngir en rolle i stedet for en person. Én konto per person, med delt makt gitt gjennom grupper, roller eller en smalt avgrenset sudo-regel, holder både loggen og avgangene ærlige.

Nettleseren bestemmer hva brukeren får gjøre. En rolle som ligger i localStorage, i en informasjonskapsel eller i et skjult skjemafelt, er et forslag fra klienten, og hvem som helst kan redigere den. Stoler serveren på den, blir redigeringen et angrep. Klienten kan godt huske kontekst for å gjøre ting lettere; serveren må sjekke tillatelsene selv, ved hver forespørsel.

En tjeneste kjører som root fordi det var enklere. Alt virker, men en feil i tjenesten som kan utnyttes, kan sette hele verten i fare. Gi hver tjeneste sin egen uprivilegerte bruker, og gi ekstra rettigheter smalt, for én navngitt kommando,

heller enn bredt.

Les mer

- NIST CSRC glossary: user — definisjonene som brukes på tvers av sikkerhetspublikasjonene fra NIST, hver med dokumentet den kommer fra.
- POSIX.1-2024 Base Definitions: Definitions — den formelle betydningen av brukerdatabase, bruker-ID og brukernavn på Unix-lignende systemer.
- RFC 7643: SCIM Core Schema — ressursen User for å flytte kontoer mellom tjenester, med `userName` , `id` og `active` .
- NIST SP 800-63-4: Digital Identity Guidelines — hvordan én person kan ha flere digitale identiteter, og rollene *applicant*, *subscriber* og *claimant*.
- POSIX.1-2024: File Access Permissions — tilgang gjennom tillatelsesklassene eier, gruppe og andre, alternative tilgangskontroller og nødvendige privilegier; eierskap alene avgrenser ikke tilgangen.

Ordliste

Velg ut fra deres faktiske rammer

Beskriv enheten eller tjenesten, observerte symptomer og dataene som må bevares. Vi kan fastslå det tryggeste nyttige undersøkelsessteget.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er en IT-bruker?» 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/user/