Engineer

Användare

person eller process för personens räkning med systemåtkomst

Vad det är

En användare är den, eller det, som ett system agerar för. I vanlig teknisk text gör ordet tre olika jobb, och det mesta av förvirringen kring användare kommer av att de jobben får flyta ihop till ett.

Den första betydelsen är personen: någon som öppnar en produkt och försöker få något gjort. Designer, supportpersonal och produktansvariga menar oftast den, och den har ingen fast form alls inne i systemet. Den andra är kontot: den post som ett system sparar för att kunna känna igen någon igen, oftast ett namn att logga in med, en intern identifierare, en uppsättning behörigheter och en status som aktiv eller avstängd. Den mesta applikationskoden menar den. Den tredje är användaren i operativsystemet: på Unix-liknande system en post i användardatabasen med ett användarnamn och ett numeriskt användar-id. Processer som kör har användar-id-uppgifter som kärnan använder för behörighetskontroller.

De tre stämmer sällan överens ett till ett. En person kan ha konton i många tjänster, och NIST:s riktlinjer för digital identitet säger rakt ut att en person kan ha flera digitala identiteter, där var och en är unik bara inom sin egen tjänst. Ett konto kan delas av flera personer, vilket nästan alltid är ett misstag. Och väldigt många användare har ingen person bakom sig alls: webbservern, databasen, jobbet för säkerhetskopiering och skriptet för driftsättning körs var och ett som en egen användare i operativsystemet, och har ofta konton i andra system också. Det är därför definitionen från NIST lyder ”individual, or (system) process acting on behalf of an individual”, alltså en individ eller en process som agerar för en individs räkning.

På en Unix-värd är det lätt att se uppdelningen mellan namn och nummer:

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

Systemkärnan arbetar med numret. POSIX definierar en användardatabas som för varje användare innehåller användarnamnet, det numeriska användar-id:t, ett första grupp-id, en första arbetskatalog och ett första program att köra. Ägarskap till filer lagras som numret, och namnet slås upp först när något ska visas för en person. En process bär dessutom mer än ett användar-id: ett verkligt, som säger vem som startade den, och ett effektivt, som säger vems behörigheter den använder just då.

Konton i applikationer gör oftast samma uppdelning. Schemat i SCIM, som används för att föra över användare från ett system till ett annat, kräver ett `userName` som människor ser och loggar in med, unikt inom tjänsten och jämfört utan hänsyn till versaler och gemener, och ett separat `id` som tjänsten tilldelar, som förblir stabilt och aldrig delas ut igen. En flagga, `active`, skiljer ett avstängt konto från ett som fungerar.

Använd begreppet i ett beslut

Använd ”Vad är en användare?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Laptopen, skrivaren, inloggningen och e-posten, fixade snabbt och på ett begripligt språk, utan att någon behöver känna sig dum.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Etablerade en avdelning för teknisk support — 10,000 kunder som fick hjälp av en supportavdelning byggd från grunden

Etablerade en avdelning för teknisk support Hör av er →

Varför det spelar roll

Varje beslut om åtkomst är ett beslut om en användare, så en grumlig bild av vem användaren är blir ett grumligt beslut. Frågan ”får den här personen se den här fakturan?” besvaras i koden som ”har det här kontot, i det här sammanhanget, en behörighet som täcker den här posten?”, och varje steg i den översättningen är ett ställe där den avsedda personen och det faktiska kontot kan glida isär.

Gränsen mellan person och konto är också platsen där ansvarsskyldigheten finns. Loggar registrerar konton. När varje konto tillhör exakt en person säger en loggrad vem som gjorde något. När ett konto delas säger loggen vilken

hemlighet som användes och ingenting om vem som skrev in den, och att stänga en persons åtkomst innebär att ändra den för alla.

Användare i operativsystemet är ett väletablerat verktyg för minsta behörighet. En tjänst som körs som en egen oprivilegierad användare begränsas av den användarens behörigheter, inte bara av filägande. Den kan fortfarande ändra delade skrivbara resurser, göra nätverksanrop och använda inloggningsuppgifter som den har tillgång till. Separata tjänsteanvändare minskar skadan vid ett intrång; de ger inte fullständig isolering. Samma tjänst körd som superanvändaren kan utsätta hela maskinen för risk. Att ge varje program en egen användare är en liten konfigurationsändring som begränsar de tillgängliga behörigheterna när något går fel.

Till sist har personer och konton olika livslängd. Personer byter namn, e-postadress och arbetsgivare, och konton stängs av, slås ihop och raderas. Ett system som behandlar ett attribut som kan ändras, t.ex. en e-postadress, som kontots identitet kommer en dag att knyta en persons historik till någon annan.

Så ser det ut i praktiken

På en maritim plattform förvaltar yrkesverksamma organisationer, som företag och akademier, som saknar egna inloggningar. Sidan säger regeln rakt ut: personen är kontot, och organisationen är något som personen agerar på uppdrag av. Arbetet var ett kontextbyte som låter en användare agera som vilken organisation som helst som den förvaltar. Webbläsarens lokala lagring håller reda på vilken organisation som är aktiv, så bytet sker direkt, och en cookie på serversidan speglar valet så att sidor som renderas på servern visar samma kontext. Åtkomsten följer ändå användaren och inte det webbläsaren minns: servern slår upp behörigheten på nytt när varje anrop kommer in, så den som redigerar det sparade värdet ändrar bara vad den egna skärmen visar.

På företagets egen värd levereras releaser av en användare i operativsystemet som nästan inte har några rättigheter alls. När containermiljön sattes upp skildes driftsättning från provisionering. Root används en gång, för att förbereda driftsättningsvägen. Varje senare driftsättning görs av den oprivilegierade användaren, som genom en avgränsad regel får köra ett enda fast skript utan argument och ingenting annat. En rutinmässig release bygger avbildningen och startar om tjänsten utan att något root-skal öppnas.

Att veta vilka användarna är blir i sig en rapport. En av sju skrivskyddade rapportroller återger en åtkomstrapport från den levande värden som Markdown i repot, med konton, sudo-omfattning, nyckelfingeravtryck, användare i git-forgen och databasroller sida vid sida. Alla sju rapporterna redovisar enbart siffror som körningen själv har mätt. Tillsammans har rapporterna hittat verkliga saker, bl.a. två döda säkerhetsåtgärder och en odeklarerad lyssnande port.

Var det går fel

En raderad användare kommer tillbaka som någon annan. Ett konto tas bort, dess identifierare delas senare ut igen, och det nya kontot ärver allt som fortfarande pekar på det gamla värdet: rader i en tabell, en plats på en lista, filer på disken. På en Unix-värd behåller de filer som en borttagen användare ägde sin numeriska ägare, och nästa användare som skapas med det numret äger dem. Ge konton identifierare som aldrig återanvänds, så som SCIM kräver av sitt `id`, och bestäm vad som händer med en avgående användares data innan användaren tas bort.

En e-postadress används som konto. Den ser ut som en naturlig nyckel tills någon byter adress, förlorar åtkomsten till en gammal eller en arbetsgivare ger en adress vidare till en ny medarbetare. Då knyts en persons historik till en annan, eller så får en person två konton. Behåll en stabil intern identifierare som nyckel och behandla adressen som ett attribut som kan ändras.

Alla loggar in med samma konto. En delad administratörsinloggning går fort att sätta upp och är omöjlig att granska. När någon slutar upphör åtkomsten bara om hemligheten ändras för alla, och loggen namnger en roll i stället för en person. Ett konto per person, där delad makt ges genom grupper, roller eller en snävt avgränsad sudo-regel, håller både loggen och avgångarna ärliga.

Webbläsaren avgör vad användaren får göra. En roll som sparas i lokal lagring, i en cookie eller i ett dolt formulärfält är ett förslag från klienten, och vem som helst kan redigera det. Om servern litar på det blir redigeringen en attack. Klienten får minnas sammanhang för bekvämlighetens skull, men servern måste själv kontrollera behörigheterna, vid varje anrop.

En tjänst kör som root för att det var enklare. Allt fungerar, men ett fel i tjänsten som går att utnyttja kan utsätta hela värden för risk. Ge varje tjänst en egen oprivilegierad användare, och ge varje extra rättighet snävt, för ett namngivet kommando, i stället för brett.

Läs mer

- NIST CSRC glossary: user — definitionerna som används i NIST:s publikationer om säkerhet, var och en med det dokument den kommer från.
- POSIX.1-2024 Base Definitions: Definitions — den formella betydelsen av user database, user ID och user name på Unix-liknande system.
- RFC 7643: SCIM Core Schema — resursen User för att flytta konton mellan tjänster, med `userName`, `id` och `active`.
- NIST SP 800-63-4: Digital Identity Guidelines — hur en person kan ha flera digitala identiteter, och rollerna applicant, subscriber och claimant.
- POSIX.1-2024: File Access Permissions — åtkomst genom behörighetsklasserna ägare, grupp och övriga, alternativa åtkomstkontroller och lämpliga privilegier; ägande ensamt avgränsar inte åtkomsten.

Ordlista

Välj utifrån era faktiska förutsättningar

Beskriv enheten eller tjänsten, observerade symtom och uppgifterna som måste bevaras. Vi kan fastställa det säkraste användbara undersökningssteget.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är en användare?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/user/