Engineer

Adgangskode

✳ en hemmelig streng, der beviser, hvem der logger ind

Hvad det er

En adgangskode er en række tegn, som en person husker eller gemmer i en password manager, og som vedkommende viser frem for at godtgøre, at kontoen er vedkommendes. Definitionerne i NIST's ordliste er enige om kernen: bogstaver, tal og andre tegn, der bruges til at autentificere en identitet eller til at bekræfte en adgangstilladelse, og i nogle dokumenter også til at aflede kryptografiske nøgler. Den gældende vejledning om digital identitet, SP 800-63-4, kalder den faktoren »noget, du ved«, og nævner, at den første udgave brugte betegnelsen memorized secret. En adgangsfrase, der består af en række ord, og en pinkode, der kun består af cifre, er begge adgangskoder i bredere forstand.

Den samme streng kan løse to opgaver, der ligner hinanden. En adgangskode, der bruges til at logge ind, sendes til en verifikator, som gemmer nok til at genkende den og aldrig bør gemme selve adgangskoden. En adgangskode, der låser noget op lokalt, bliver på enheden. SP 800-63B kalder den slags en activation secret, og det typiske eksempel er pinkoden til en autentifikator med flere faktorer: den bruges på enheden til at nå den hemmelighed, autentifikatoren gemmer.

Vanskeligheden er, at en adgangskode er en delt hemmelighed. Brugeren kender den, tjenesten skal kunne genkende den, og enhver, der får den at vide, kan bruge den præcis som brugeren. Intet i strengen binder den til det site, der bad om den, og derfor skriver SP 800-63B ligeud, at adgangskoder ikke er phishingresistente. Det meste af ingeniørarbejdet omkring adgangskoder handler om at begrænse, hvad den delte viden koster, når den slipper ud.

Brug begrebet i en beslutning

Brug »Hvad er en adgangskode?« 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

En adgangskode er ofte det eneste, der står vagt om en konto. To slags gætteri har betydning, og hver af dem holdes tilbage af noget forskelligt.

Online gætteri vil sige at prøve adgangskoder mod den aktive loginformular, og dér bestemmer tjenesten tempoet. SP 800-63B sætter loftet for fejlslagne forsøg i træk med én autentifikator på én konto til 100 og kræver, at nye adgangskoder tjekkes mod en blokeringsliste over almindelige, forventelige og lækkede værdier, så de valg, en angriber ville prøve først, aldrig bliver godkendt.

Offline gætteri begynder, når en kopi af de gemte adgangskodedata har forladt bygningen. Så er der ingen formular og intet loft. Vejledningen bemærker, at angribere kan beregne mange milliarder hashes i sekundet offline, og at adgangskoder, der skal klare det, må være flere størrelsesordener mere komplekse end dem, der kun møder en loginformular. Derfor er det lagringen, der afgør udfaldet. SP 800-63B kræver, at adgangskoder saltes og hashes med et skema til hashing af adgangskoder, som tager adgangskoden, et salt og en omkostningsfaktor og findes for at gøre hvert gæt dyrt. Saltet skal være mindst 32 bit og vælges, så saltværdier sjældent falder sammen, og det forhindrer, at to konti med samme adgangskode deler en gemt hash. Omkostningsfaktoren skal være så høj, som verifikatoren har råd til, og hæves med tiden. Vejledningen anbefaler også at notere, hvilket skema og hvilken omkostning der lavede hver hash, så systemet senere kan skifte til et stærkere.

RFC 9106 beskriver Argon2, en hukommelsestung funktion bygget til netop den opgave, og anbefaler varianten Argon2id: én gennemgang over 2 GiB hukommelse som standard i alle miljøer eller tre gennemgange over 64 MiB, hvor der er knap hukommelse. RFC'en skriver, at den første indstilling maksimerer en angribers omkostninger på dedikeret hardware til brute force – den egenskab, der tæller, når en fil med hashes er lækket. OWASP Password Storage Cheat

Sheet giver lavere brugbare minimumsværdier og alternativer til systemer, der ikke kan bruge Argon2id, og fastslår reglen under dem alle. Hurtige hashfunktioner som SHA-256 egner sig ikke, fordi de lader en angriber gætte meget hurtigt, og adgangskoder hashes i stedet for at blive krypteret, fordi kryptering virker begge veje, så originalen kan hentes frem igen.

Sådan ser det ud i praksis

Før et fælles system til håndtering af adgangskoder blev indført i hele virksomheden, lagrede og delte hver især adgangsoplysningerne på sin egen måde. Siden beskriver, hvordan det ser ud i hverdagen: sjældent et dramatisk brud, oftere en adgangskode i en chatbesked, et delt login, som ingen nogensinde skifter adgangskode på, og en langsom ophobning af små eksponeringer. Systemet gav organisationen én ensartet måde at lagre og dele oplysningerne på, og sidens pointe er, at det ikke var op til den enkelte, for en password manager, som kun halvdelen af teamet bruger, hjælper knap nok, når risikoen ligger i den halvdel, der lader være. Da oplysningerne først lå ét centralt administreret sted, blev adgangskontrollen enklere og mere konsistent. SP 800-63B peger samme vej fra tjenestens side: verifikatorer skal tillade password managers og autoudfyldning og bør tillade indsætning, og vejledningen nævner en password manager som måden at holde en særskilt adgangskode til hver tjeneste på.

Da endnu en server blev oprettet fra kode, leverede den første maskines historie argumentet. Den var oprettet manuelt og dens firewall tilføjet bagefter, og det efterlader et tidsvindue, hvor en helt ny vært med en standardpolitik for adgangskoder kan nås fra internettet. Løsningen er rækkefølgen: den nye maskine fødes bag sin firewall, fordi firewall-playet kører før server-playet.

Ved et login hos en stor mailudbyder fortalte programmet brugeren, at adgangskoden var forkert. Det var den ikke. Udbyderen kræver en programspecifik adgangskode til tredjepartsklienter, så én konto havde to slags adgangskoder, og en besked, der kun kendte til den ene, sendte brugeren ud i at genindtaste noget, der aldrig kunne virke. Den omskrevne besked nævner udbyderen, oplyser, at den kræver en programspecifik adgangskode, og siger, hvor man opretter en, og en test tjekker udbyderens navn og typen af adgangsoplysninger.

Hvor det går galt

Én adgangskode til mange konti. Når den samme adgangskode beskytter flere tjenester, åbner et brud hos den svageste for resten. SP 800-63B kalder det password stuffing: en adgangskode, der er taget fra ét site, bruges mod den samme persons konti på andre sites. Brugerne forsvarer sig med en særskilt adgangskode til hver tjeneste, i praksis via en password manager, og tjenesterne ved at tjekke nye adgangskoder mod værdier fra tidligere brud.

Regler, der gør adgangskoder svagere. Krav til sammensætning føles strenge og giver forudsigelige resultater. Vejledningens eget eksempel er en bruger, der ville have valgt »password«, og som vælger »Password1«, når der kræves et stort bogstav og et ciffer, og »Password1!«, når der også kræves et symbol. Den udelukker regler for sammensætning, planlagte skift, hints, der kan læses før login, og sikkerhedsspørgsmål som navnet på det første kæledyr, og den kræver stadig et skift, så snart der er tegn på, at adgangskoden er kompromitteret.

En hurtig hash, eller ét salt til alle rækker. En tabel med adgangskoder, der er hashet med en generel funktion eller saltet med den samme værdi hele vejen igennem, giver en angriber offline billige gæt, der kan prøves mod alle konti på én gang. Systemer, der arver gamle hashes, kan hashe hver adgangskode igen med det nye skema, næste gang brugeren logger ind, som OWASP's cheat sheet beskriver, og den gemte reference til det anvendte skema viser, hvilke rækker der stadig står på det gamle.

Adgangskoden bliver kortet af eller kan ikke indsættes. SP 800-63B kræver, at hele den indsendte adgangskode verificeres og aldrig kun en afkortet del, og vil have indsætning tilladt, så password managers virker, hvor autoudfyldning ikke gør. Nogle hashfunktioner har deres egen grænse: OWASP's cheat sheet bemærker, at bcrypt i de fleste implementeringer højst tager 72 byte input, og beder tjenester, der bruger den, om at håndhæve det maksimum.

Adgangskoden ligger et sted, den aldrig skulle have været. En adgangskode, der er sat ind i en chat, skrevet i en sag eller udskrevet i en log, er en kopi uden for alle de kontroller, det rigtige lager har. Den eneste måde at tage kopien tilbage på er at skifte adgangskoden, og derfor betyder ét administreret sted mere end nogen regel om, hvordan adgangskoden ser ud.

Læs mere

- Password i NIST CSRC's ordliste — definitioner fra FIPS 140-2, SP 800-63-4 og andre, med adgangsfrasen som et særtilfælde.
- NIST SP 800-63B-4 — de gældende regler for at vælge, tjekke og gemme adgangskoder, med begrundelserne i bilag A.
- RFC 9106 — Argon2, med de to anbefalede indstillinger af Argon2id til hashing af adgangskoder.
- OWASP Password Storage Cheat Sheet — brugbare parametre for Argon2id, scrypt, bcrypt og PBKDF2, og hvordan gamle hashes opgraderes.

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 en adgangskode?« 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/password/