CONSCIA MULTI-FACTOR AUTHENTICATION

Med MFA kan I være helt sikre

conscia

Multi-Factor Authentication (MFA) i en kontekst

Organisationer bliver, og er det i mange tilfælde allerede, kompromitteret. Paradigmet om at angriberne bliver stoppet ved perimeteren gælder ikke længere. Angriberne opererer nu på indersiden forklædt som almindelig bruger - og i værste tilfælde som administrator med udvidede rettigheder til alle systemer.

Derfor anbefales det i dag at anvende systemer, der validerer brugerne baseret på flere faktorer – Multi-Factor Authentication. MFA kombinerer to eller flere uafhængige legitimationsoplysninger: Hvad brugeren ved (adgangskode), hvad brugeren har (sikkerhedstoken) og hvad brugeren er (biometrisk verifikation).

MFA's mål er at skabe sikkerhed i flere lag og gøre det vanskeligere for en uautoriseret person at få adgang til et mål, såsom en fysisk placering, computerenhed, netværk eller database. Hvis en faktor er kompromitteret eller ødelagt, har angriberen stadig mindst én barriere mere at skulle bryde, før der med succes kan nåes ind til målet.

Oftest ses kun 2-faktor autentifikation anvendt, hvor man benytter adgangskode sammen med, hvad brugeren har eller, hvad brugeren er. Brugen af MFA nedsætter sikkerhedsrisikoen signifikant, og det er en anbefalet kontrol i fx CIS-kontrollerne at anvende MFA både for administratorer, men også for almindelige brugere.

Conscia og MFA

Conscia tilbyder MFA som en service. Det betyder, at vi håndterer infrastrukturen bag løsningen. Løsningen er baseret på Duo Securitys cloud-løsning.

Med Conscias MFA-as-a-Service får I en af de stærkeste løsninger på markedet:

- Høj grad af bekvemmelighed
- Risikoreduktion
- Høj ydeevne
- Nem distribution uden installation

Løsningen reducerer risici via sine høje standarder for sikkerhed og stabilitet. Platformen er bygget med sikkerhed for øje. Den anvender asymmetrisk kryptering for at verificere de enkelte enheder mod løsningens systemer, hvilket gør det vanskeligt for angribere at kompromittere enhederne.

Platformen anvender 2-faktor autentifikation, som gør det muligt for brugere, der har indtastet adgangskoder at verificere deres identitet ved hjælp af en anden faktor. Dette afværger mand-i-midten-angreb (MITM), hvor en ondsindet aktør forsøger at kapre en login-session og stjæle adgangskoder. Derudover har løsningen flere offsite-sikkerhedskopier af kundedata i tilfælde af systemstop eller andre fejl. Løsningen understøtter i dag en række høje standarder for sikkerhed, som f.eks. PCI DSS, ISO 27001, OWASP og NIST 800.

Duo sikrer desuden en oppetid for leveranceplatformen, der overstiger 99.995%, med garanti for serviceniveauet.

conscia

6 vigtige funktioner

1 Let at anvende for alle brugere

Duos mange forskellige godkendelsesmetoder gør det nemt for alle brugere at logge sikkert og hurtigt ind. Duo Push, sendt fra Duo Mobile-appen, giver brugerne mulighed for at godkende push-meddelelser til at verificere deres identitet. Løsningen understøtter også Universal 2nd Factor (U2F) sikkerhed, hardware tokens, mobile adgangskoder, SMS, telefonopkald og biometri som f.eks. Touch ID for at give meget fleksible muligheder for alle typer brugere.

2 Let opsætning og provisionering af brugere

Med Duo kan brugerne let konfigurere deres app på en intuitiv måde. Løsningen tilbyder bl.a. en automatiseret udrulning for at lette provisionering i større organisationer. Højere sikkerhed opnås hurtigt ved hjælp af let synkronisering af tusinder af brugere fra eksisterende Active Directory, Azure AD eller import via et API.

3 Reducerer omkostning til helpdesk

Selvservice giver brugeren mulighed for let at administrere deres egne enheder i forbindelse med login uden at skulle anvende en separat portal eller kontakte helpdesk, når de får en ny mobilenhed.

4 Sikring af alle applikationer

Med MFA-as-a-Service baseret på Duo Security kan man sikre både on-prem og cloud-applikationer. Løsningen har et bredt partnerlandskab, der sikrer en øget sikkerhed for enhver applikation og service herunder Office365, Amazon Web-Services, Palo Alto Networks Firewall, Palo Alto Networks Global Protect, Cisco AnyConnect og mange flere.

5 Validering af End-User-identitet

Duo Help Desk Push gør det muligt for fx administratorer og helpdesk at validere brugerens identitet med Duo Push, før en ændring udføres, når brugeren beder om dette. Duo Help Desk Push hjælper med at validere, at brugeren er dén, vedkommende udgiver sig for at være.

6 Hurtig udrulning og skalering

Implementering selv i stor skala har aldrig været så let. Duos SaaS løsning kræver minimal infrastruktur for at kunne rulles ud til tusinder af brugere. Derudover kan løsningen sende opdateringer til brugernes enheder for at sikre, at de altid har den seneste sikkerhedspatch og funktioner.

Vil du høre mere om MFA?

Kontakt Nikolaj Andersen Wølck, Security Architect
Mail: naw@conscia.com
Mobil: +45 51 80 54 10