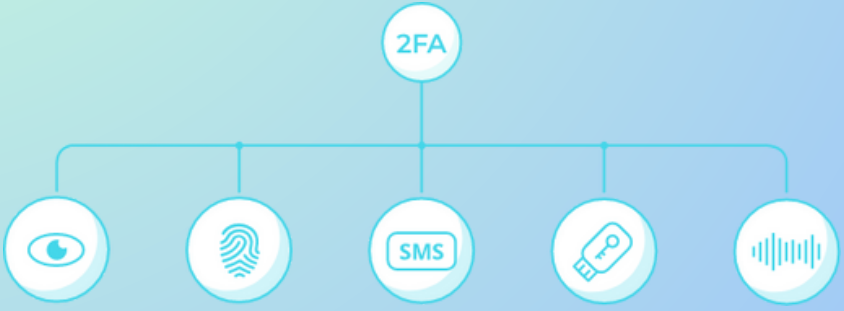
Dvofaktorska i multifaktorska autentifikacija



CIRT.ME

Kompleksna lozinka nije dovoljna za sigurnost naših naloga!

Šta je dvofaktorska autentifikacija (2FA)?

Dvofaktorska autentifikacija je dodatni sloj sigurnosti koji štiti vaše naloge.

Uz lozinku, koristi se još jedan faktor, kao što je generisani kod putem mobilne aplikacije, SMS poruka, otisak prsta i slično.

Ova dodatna zaštita otežava hakovanje naloga čak i ako neko zna vašu lozinku.

Kombinacija onoga što znate (lozinka) i onoga što posjedujete (mobilni uređaj, biometrija) čini vaš nalog mnogo sigurnijim.

Vrste dvofaktorske autentifikacije

- SMS kodovi: Kodovi za autentifikaciju se šalju korisniku putem SMS poruke na registrovani mobilni uređaj.
- Biometrija: Podrazumijeva autentifikaciju putem otiska prsta, prepoznavanja lica ili skeniranja rožnjače oka.

Vrste dvofaktorske autentifikacije

- Aplikacije za autentifikaciju: U pitanju su mobilne aplikacije koje generišu vremenski ograničene kodove (npr. Google Authenticator, Authy).

- Tokeni: Ako koristite softverske ili fizičke tokene, čuvajte ih na sigurnom mjestu. Fizički tokeni trebaju biti pažljivo čuvani, dok bi mobilni uređaj sa softverskim tokenom trebao biti zaštićen dodatnom lozinkom ili biometrijom.

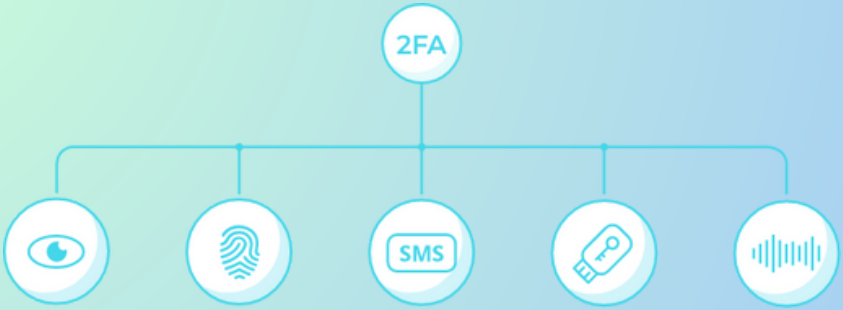
Multifaktorska autentifikacija (MFA)

Multifaktorska autentifikacija (MFA) je sigurnosni postupak koji koristi tri ili više nezavisna načina identifikacije.

Ovaj pristup ima za cilj povećati sigurnost autentifikacije dodajući više slojeva zaštite.

MFA koristi kombinaciju faktora iz tri glavne gore navedene kategorije: nešto što znate, nešto što jeste I nešto što posjedujete.

Kombinacijom ovih faktora, MFA pruža dodatni sloj sigurnosti jer neovlašćenim osobama postaje izuzetno teško prevazići sve identifikacione barijere.



CIRT.ME