Beveiligingsmaatregelen

In dit beleidsdocument worden de beveiligingsmaatregelen omschreven die Genkgo in haar software systemen heeft getroffen. Deze maatregelen zijn niet statisch. Het invoeren van nieuwe beveiligingstechnologie kan leiden tot een verbeterd beveiligingsniveau. Daarom zijn beveiligingsmaatregelen onderhevig aan verandering. Anderzijds kunnen in technologieën bepaalde kwetsbaarheden worden gevonden die ertoe leiden dat bepaalde beveiligingsmechanismes niet meer adequaat zijn. Tot slot kan Genkgo besluiten haar dienstverlening uitbreiden. Nieuwe dienstverlening kan ertoe leiden dat de beveilgingsmaatregelen dienen te worden uitgebreid.

Op deze locatie worden de maatregelen beschreven zoals deze op dit moment worden getroffen.

- Genkgo versleutelt verbindingen waarover persoonsgegevens worden verzonden door middel van HTTPS.
- Genkgo beveiligt haar administratieve software met gebruikerverificatie. Verificatie geschiedt door een gebruikersnaam en wachtwoord, waarbij aan het wachtwoord eisen worden gesteld om deze sterk genoeg te laten zijn.
- Genkgo stelt beheerders in staat bepaalde delen van de administratieve software af te sluiten voor andere beheerders door middel van een rollensysteem.
- Genkgo stelt de beheerder in staat delen van websites en apps te beveiligen met gebruikerverificatie. Ook deze verificatie geschiedt door een gebruikersnaam en wachtwoord, waarbij aan het wachtwoord eisen worden gesteld om deze sterk genoeg te laten zijn.
- Genkgo stelt de beheerder in staat bestanden te beveiligen met gebruikerverificatie.
- Genkgo draagt zorg voor een adequate hash-methode bij het opslaan van wachtwoorden.
- Genkgo treft maatregelen om code injectie te voorkomen. Daaronder wordt in ieder geval verstaan maar is niet gelimiteerd tot SQL injectie, XSS en objectinjectie. Hiertoe heeft Genkgo meerdere lagen van beveiliging geactiveerd.
- Genkgo treft maatregelen om haar servers te beschermen tegen inbrekers.
- Genkgo treft maatregelen om gebruikers te beschermen tegen het stelen van hun gebruikerssessies.
- Genkgo treft maatregelen om authenticiteit van verzonden e-mail berichten te waarborgen.
- Genkgo draagt zorg voor het frequent bijwerken van de gebruikte software op haar platform naar de laatste stabiele versies.
- Genkgo laat een derde partij ten minste jaarlijks beveiligingstesten uitvoeren op haar software platform en zal zorgdragen voor adequate opvolging indien bepaalde kwetsbaarheden worden gevonden.
- Genkgo draagt zorg voor het bijwerken van kennis en kunde van haar personeel omtrent software beveiliging.
- Genkgo slaat data op in datacentra die beschikken over een ISO 27001:2013 certificaat. Hiervoor gebruikt Genkgo onderaannemers.

Dit document is voor het laatst aangepast op 24 sep 2020 om 13:35:57.