



Security

Centric beleid informatiebeveiliging

Centric heeft een informatiebeveiligingsbeleid opgesteld waarin de uitgangspunten en stuurmechanismen benoemd zijn voor een veilige verwerking van gegevens. Het beleid is uitgewerkt in concrete procedures en maatregelen.

Secure Software Development

De basis voor security ligt bij de ontwikkeling van veilige software. Centric gebruikt hiervoor de methode en normenkaders van Secure Software Development (SSD) van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Wij passen daarbij de methode Grip op SSD toe, hierdoor hebben klanten inzicht in onze werkwijze voor het ontwikkelen van veilige software. De security requirements van SSD zijn opgenomen in de Centric Baseline voor secure software development en zijn voorwaarde bij de (door)ontwikkeling van onze software.

Security audits en pentesten

Centric heeft een eigen team van ethical hackers (het Red Team) dat structureel security audits en pentesten uitvoert op onze softwareproducten en -diensten. Bij het testen wordt onder andere gebruik gemaakt van de SSD-normenkaders, de Top 10 Application Security Risks van Open Web Application Security Project (OWASP) en de Nationaal Cyber Security Centrum (NCSC) ICT-Beveiligingsrichtlijnen voor Webapplicaties en mobiele applicaties. De bevindingen van deze pentests leiden tot aanpassingen binnen onze software. Gevonden kwetsbaarheden worden beoordeeld op impact en kans. Op basis van het risico wordt de prioriteit bepaald en worden de kwetsbaarheden verholpen.

DigiD-assessments

Logius vereist een jaarlijks ICT-beveiligingsassessment voor applicaties die DigiD gebruiken. Voor deze assessment heeft Logius een normenkader opgesteld. De toetsing moet worden uitgevoerd door een Register EDP-auditor. Voor de betreffende applicaties laat Centric jaarlijks een externe auditor een assessment uitvoeren voor het applicatiegedeelte en het hostingsgedeelte. De Third Party Mededeling (TPM) die we aan onze klanten ter beschikking stellen dekt hiervoor relevante normen af. Elke klant moet daarnaast een audit op het eigen securitybeleid laten uitvoeren. Onze TPM kan samen met het gedeelte van de klant bij Logius ter verificatie worden aangeboden.

ISO 27001 Certificering clouddiensten

Centric heeft voor de levering van (cloud)diensten een informatiebeveiligingsbeleid opgesteld en geïmplementeerd conform de beveiligingsnorm ISO 27001. De beheeractiviteiten die worden uitgevoerd voor clouddiensten zijn volgens deze norm gecertificeerd. Op basis van jaarlijkse risicobeoordelingen, audits, wijzigingen in wet- en regelgeving en business requirements scherpen we ons informatiebeveiligingsbeleid continu aan.

