Vertrouwelijkheid en integriteit

Digitaal Loket Toezicht (DLT)

In dit document wordt de werking van het Digitaal Loket Toezicht (DLT) toegelicht en worden de maatregelen besproken die De Nederlandsche Bank (DNB) heeft getroffen om van het DLT een veilige en betrouwbare omgeving voor aanvragen te maken.

De Wet op het financieel toezicht en andere wet- en regelgeving schrijven voor dat ondernemingen die willen toetreden tot de financiële markt hiervoor meestal toestemming nodig hebben, bijvoorbeeld in de vorm van een vergunning. Een vergunning kan bij DNB worden aangevraagd.

DNB toetst of (beoogd) bestuurders en commissarissen geschikt zijn om hun functie te vervullen en of hun betrouwbaarheid buiten twijfel staat. Zij kunnen daarbij gebruikmaken van het aanvragensysteem DLT dat DNB beschikbaar stelt. Het DLT maakt gebruik van het internet om gegevens tussen DNB en de aanvrager uit te wisselen. De gegevens die de instellingen aan DNB aanleveren zijn vertrouwelijk, terwijl internet een openbaar netwerk is. Het is duidelijk dat deze combinatie risico's met zich meebrengt. DNB heeft daarom op verschillende vlakken maatregelen genomen om de vertrouwelijkheid en integriteit van gegevens te waarborgen.

Het gebruik van encryptie bij de verbinding

Encryptie voorkomt dat een derde partij de informatie kan lezen die DNB en de rapporteur uitwisselen.

Het gebruik van sterke authenticatie

Met authenticatie kunnen zowel DNB als de aanvrager ondubbelzinnig vaststellen met welke partij zij gegevens uitwisselen. Het DLT-systeem gebruikt hiervoor eHerkenning, niveau 3 (tweefactorauthenticatie).

Een beveiligde infrastructuur

Het DLT-systeem is een zogenaamd client-server systeem. De computer en webbrowser van de rapporteur vormen de cliëntomgeving. De DLT-applicatie en de computer waarop deze draait vormen de serveromgeving. DNB heeft in de serveromgeving maatregelen genomen om de vertrouwelijkheid en integriteit van het aanvragensysteem te waarborgen. Het is de verantwoordelijkheid van de gebruiker om de nodige beveiligingsmaatregelen op de cliënt te nemen.

De invloed van DNB op de cliëntomgeving is beperkt

Het DLT bewaart daarom, behalve informatie voor de authenticatie, nooit gegevens op de cliëntomgeving maar altijd op de serveromgeving. Dit geldt ook voor aanvragen die nog niet zijn ingediend. Hierdoor kan DNB voldoende maatregelen nemen om de opgeslagen gegevens te beveiligen. Medewerkers van DNB kunnen een aanvraag overigens pas inzien nadat zij is ingediend. DNB verzekert zich er periodiek van dat alleen op de door haar bedoelde wijze toegang kan worden verkregen tot de DLT-server. Jaarlijks voeren we beveiligingsassessments uit (waaronder pentesten). De conclusies van dit periodiek onderzoek gebruikt DNB zo nodig om haar systeem verder te verbeteren. DNB heeft een responsible disclosure voor het geval een gebruiker toch een kwetsbaarheid aantreft.

Veiligheidsprocedures

DNB gebruikt verschillende procedures om de veiligheid van het DLT-systeem verder te verhogen. Slechts een beperkt aantal DNB-systeembeheerders heeft toegang tot het systeem. Bovendien wordt het gebruik van het systeem gelogd. Misbruik van buitenaf wordt gemonitord. Indien misbruik wordt waargenomen neemt DNB tegenmaatregelen. Zo nodig legt DNB het systeem tijdelijk stil. DLT verbreekt de verbinding met een aanvrager indien er gedurende enige tijd geen activiteit heeft plaatsgevonden.

Risicobewustzijn

Integriteit is één van de kernwaarden van DNB en heeft haar constante aandacht. De medewerkers en het management van DNB zijn zich bewust van hun verantwoordelijke positie in de maatschappij en handelen hiernaar. Tevens beseft DNB dat wat gisteren veilig was dat morgen niet meer hoeft te zijn. Daarom toetst en evalueert zij periodiek alle hierboven genoemde maatregelen.

DeNederlandscheBank
EUROSYSTEEM