Vertrouwelijkheid en integriteit

Digitaal Loket Rapportages (DLR)

In dit document wordt de werking van het Digitaal Loket Rapportages (DLR) toegelicht en worden de maatregelen besproken die De Nederlandsche Bank (DNB) heeft getroffen om van het DLR een veilige en betrouwbare rapportageomgeving te maken.

De Wet op het financieel toezicht en andere wet- en regelgeving schrijven voor dat onder toezicht staande instellingen hun periodieke verslaglegging aan DNB elektronisch aanleveren. Zij dienen daarbij gebruik te maken van het rapportagesysteem DLR dat DNB beschikbaar stelt. Het DLR maakt gebruik van het internet om gegevens tussen DNB en de rapporteur uit te wisselen. De gegevens die de instellingen aan DNB rapporteren 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 rapporteur ondubbelzinnig vaststellen met welke partij zij gegevens uitwisselen. Het DLR systeem gebruikt hiervoor eHerkenning, niveau 3 (2 factor authenticatie).

Een beveiligde infrastructuur

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

De invloed van DNB op de cliëntomgeving is beperkt.

Het DLR bewaart daarom, behalve informatie t.b.v. de authenticatie, nooit gegevens op de cliëntomgeving maar altijd op de serveromgeving. Dit geldt ook voor rapportages die niet zijn aangeleverd. Hierdoor kan DNB voldoende maatregelen nemen om de opgeslagen gegevens te beveiligen. Medewerkers van DNB kunnen een rapportage overigens pas inzien nadat ze is aangeleverd. DNB verzekert zich er periodiek van dat alleen op de door haar bedoelde wijze toegang kan worden verkregen tot de DLR 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 DLR 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 tegen-maatregelen. Zo nodig legt DNB het systeem tijdelijk stil. DLR verbreekt de verbinding met een rapporteur 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.

Versie 1 - 10 02 2016

DeNederlandscheBank
EUROSYSTEEM