Vertrouwelijkheid, integriteit en waarmerken

In dit document wordt de werking van e-Line DNB toegelicht en worden de maatregelen besproken die De Nederlandsche Bank (DNB) heeft getroffen om van e-Line DNB een veilige en betrouwbare rapportageomgeving te maken. De methode van waarmerken en het gebruik van attachments worden in detail besproken.

De Wet op het financieel toezicht en andere wet- en regelgeving schrijven voor dat onder toezicht staande instellingen hun periodieke verslaglegging aan DNB elektronisch indienen. Zij dienen daarbij gebruik te maken van het rapportagesysteem e-Line DNB dat DNB beschikbaar stelt. E-Line DNB 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. Encryptie voorkomt dat een derde partij de informatie kan lezen die DNB en de rapporteur uitwisselen. Het e-Line systeem gebruikt hiervoor een zogenaamde Secure Socket Layer (SSL3) die bijvoorbeeld ook gebruikt wordt bij internetbankieren.
- Het gebruik van authentificatie. Met authentificatie kunnen zowel DNB als de rapporteur ondubbelzinnig vaststellen met welke partij zij gegevens uitwisselen. Het e-Line systeem gebruikt hiervoor een Public Key Infrastructure (PKI) van Entrust. PKI wordt bovendien gebruikt om vast te stellen dat de (door encryptie onleesbare) data die DNB en de rapporteur uitwisselen niet onderweg gemanipuleerd zijn.
- Een beveiligde infrastructuur. Het e-Line systeem is een zogenaamd client-server systeem. De computer en webbrowser van de rapporteur vormen de cliëntomgeving. De e-Line applicatie en de computer waarop deze draait vormen de serveromgeving. DNB heeft zowel in de cliënt- als aan de serveromgeving maatregelen genomen om de vertrouwelijkheid en integriteit van het rapportagesysteem te waarborgen.
- De invloed van DNB op de cliëntomgeving is in principe gering. e-Line DNB bewaart daarom nooit gegevens op de cliëntomgeving maar altijd op de serveromgeving. Dit geldt ook voor rapportages die niet zijn ingediend. Hierdoor kan DNB voldoende maatregelen nemen om de opgeslagen gegevens te beveiligen. Medewerkers van DNB kunnen een rapportage overigens pas inzien nadat ze is ingediend. DNB verzekert zich er periodiek van dat alleen op de door haar bedoelde wijze toegang kan worden verkregen tot de e-Line server. Jaarlijks probeert een gespecialiseerd extern bureau met alle bekende en minder bekende technieken toegang te krijgen tot het e-Line systeem. De conclusies van dit periodiek onderzoek gebruikt DNB zonodig om haar systeem verder te verbeteren. Overigens is het tot nu toe onmogelijk gebleken om op ongeautoriseerde wijze toegang tot e-Line DNB te krijgen. De serveromgeving van het e-Line systeem heeft DNB geïsoleerd van haar overige ICT systemen. Hierdoor is het aantal systeembeheerders dat direct of via omwegen toegang heeft tot e-Line tot een minimum beperkt. Bovendien is deze server zodanig geconfigureerd dat de beveiliging maximaal is en dat er naast e-Line geen andere software kan draaien die de integriteit van het e-Line systeem mogelijk zou kunnen aantasten. De interne accountantsdienst van DNB onderwerpt het e-Line systeem geregeld aan een integriteitsonderzoek.
- Veiligheidsprocedures. DNB gebruikt verschillende procedures om de veiligheid van het e-Line systeem verder te verhogen. Bij het vorige punt is reeds genoemd dat slechts een beperkt aantal DNB systeembeheerders toegang heeft tot het e-Line systeem. In de toekomst zal bovendien elk gebruik van het systeem door medewerkers van DNB gelogd worden. Misbruik van buitenaf wordt direct opgemerkt door een zogenoemd Intrusion Detection System. Indien misbruik wordt waargenomen neemt DNB tegenmaatregelen. Zonodig legt DNB het systeem tijdelijk stil. Het e-Line systeem draait alleen tijdens kantooruren zodat mogelijk misbruik altijd direct door een medewerker wordt opgemerkt. Tot slot verbreekt e-Line 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.

Een elektronische rapportage vraagt ook om een elektronische manier van waarmerken. Indien er naast een elektronische gegevensstroom ten behoeve van het rapporteren een papieren gegevensstroom zou bestaan ten behoeve van het waarmerken, zou dit niet alleen inefficiënt zijn maar ook extra veiligheidsrisico's met zich mee brengen. Het object van waarmerken is dan ook de elektronische rapportage en niet een afdruk daarvan.
De beroepsregels van accountants schrijven voor dat de accountantsverklaring op papier wordt verstrekt. DNB heeft ervoor gekozen de koppeling tussen de papieren verklaring en de elektronische rapportage via een controlegetal te leggen. Het controlegetal is een sterk ingedikte representatie van alle in een rapportage opgenomen gegevens, inclusief de inhoud van de ingesloten bestanden. Met het indikken is alle betekenis van de gegevens verloren gegaan, het controlegetal zelf is daardoor niet vertrouwelijk. Het controlegetal heeft daarnaast andere belangrijke eigenschappen die het geschikt maken voor waarmerking. Het verandert altijd als de achterliggende gegevens veranderen en kleine veranderingen in de achterliggende gegevens leiden tot een grote verandering in het controlegetal. Alleen indien twee rapportages exact gelijk zijn zal het controlegetal van beide rapportages overeenkomen.
Elke keer dat in e-Line DNB een rapportage wordt opgeslagen zal ook het controlegetal opnieuw worden berekend. Nadat een rapportage aan DNB is verzonden, kan ze nog wel ingezien maar niet langer veranderd worden, noch door de rapporteur, noch door DNB. Het controlegetal kan daarom na verzending ook niet meer veranderen.
Het controlegetal is opgenomen op een van de staten waaruit de rapportage bestaat. Deze staat kan afgedrukt worden, desgewenst op het briefpapier van de accountant. De accountant kan deze staat vervolgens ondertekenen en naar DNB sturen. De accountant kan, in afwijking van het bovenstaande, het controlegetal ook opnemen in zijn verklaring en deze ondertekend naar DNB sturen. DNB zal het op schrift gestelde controlegetal vergelijken met dat van de elektronisch ingezonden rapportage. Indien beide overeenkomen is het voor DNB duidelijk dat ze dezelfde rapportage heeft ontvangen als die waarvoor de accountant heeft getekend. DNB, en de wet, beschouwen de rapportage dan als gewaarmerkt.
Er zijn situaties denkbaar waarin de rapporteur of DNB een herrapportage noodzakelijk acht. Hiervoor is het noodzakelijk dat DNB de rapportage opnieuw openstelt: de rapporteur kan niet zonder overleg met DNB een herrapportage indienen. De herrapportage zal bij indiening opnieuw van een verklaring voorzien moeten zijn en gewaarmerkt moeten worden. Indien de verklaring of waarmerking achterwege blijft heeft de rapporteur niet aan zijn rapportageverplichting voldaan en kan DNB sanctiemaatregelen nemen.

Overigens kent elke staat in een rapportage ook zijn eigen controlegetal. Dit duidt DNB aan met de technische term hashcode om het te onderscheiden van het controlegetal dat voor het waarmerken gebruikt wordt. De hashcodes van de te waarmerken staten worden samen met het controlegetal afgedrukt op het waarmerkformulier. Ze worden bovendien bij het afdrukken van de rapportage ook onderaan elke staat afgedrukt. Het is hierdoor altijd mogelijk veranderingen in de rapportage tot individuele staten te herleiden.

Het is mogelijk om in een rapportage complete bestanden in te sluiten. Deze worden net als in het e-mail verkeer attachments genoemd. Attachments zijn onderdeel van een rapportage en voldoen aan alle regels die ook voor andere gegevens in een rapportage gelden: ze kunnen na inzending nog wel ingezien maar niet meer gewijzigd worden, ze zijn onderdeel van het waarmerken en ze worden meegenomen bij het bepalen van het controlegetal en de hashcodes. Elke wijziging in een attachment leidt dus tot een ander controlegetal.

Bij het afdrukken van een rapportage worden attachments niet meegenomen. Een attachment zal eerst moeten worden geopend in het systeem waarmee het is aangemaakt voordat het kan worden afgedrukt. Er zal dan bovendien geen hashcode op elke pagina van het attachment worden afgedrukt.
Aan de hand van het controlegetal en de hascodes kan vastgesteld worden of twee rapportages verschillende attachments gebruiken. Het is echter niet mogelijk om aan de hand van een controlegetal of hashcode vast te stellen of een afgedrukt attachment gelijk is aan het in de rapportage ingesloten bestand. Dit kan alleen door een inhoudelijke vergelijking van de afdruk met het via e-Line DNB geopende bestand.