Factsheet Inkoopeisen Cybersecurity Overheid (ICO)

Inleiding

Digitale veiligheid is een essentiële randvoorwaarde voor vertrouwen in onze digitale economie en samenleving. De overheid heeft ervoor gekozen een samenhangend niveau van veiligheid na te streven door in alle geledingen de op ISO27002 gebaseerde 'Baseline Informatiebeveiliging Overheid' (de BIO) te hanteren.

Ook in haar inkoopbeleid wil de overheid een lijn trekken met als doel de (vele) hardware- en softwareproducten en -diensten die zij op de markt verwerft, veilig te doen zijn. De overheid ziet het als haar taak goed voorbeeld te geven, haar rol als goed opdrachtgever te versterken en daarmee ook een algemene beweging in de markt te stimuleren naar het ontwikkelen en aanbieden van veilige ICT-producten en diensten. Het programma ICO levert instrumentarium om deze doelstellingen te helpen verwezenlijken: sets van inkoopeisen, een basisprocesbeschrijving en een 'wizard' waarmee voor specifieke aanbestedingen/inkopen relevante eisen kunnen worden geselecteerd.

Waarom specifieke cybersecuritycriteria voor leveranciers?

De BIO is gericht op overheidsorganisaties. Voor eisen die overheidsorganisaties aan veilige producten van leveranciers stellen, is de BIO te breed omdat het allerlei facetten bevat die alleen op de processen van de eigen organisatie betrekking hebben. Daarnaast is de BIO te weinig specifiek voor het stellen van scherpe eisen aan de veiligheid op het niveau van ingekochte producten en diensten van leveranciers. De noodzaak om die scherpere eisen te stellen heeft geleid tot verdiepende, naar thema's georiënteerde uitwerkingen, die steunen op de BIO-normen en blinde vlekken daarin aanvullen met gebruikmaking van normen uit de andere marktstandaards.

Het fundament van de ICO-Wizard

De eisen in de wizard zijn gebaseerd op de BIO (ISO27002). De BIO vormt de basis voor nadere uitwerkingen naar samenhangende thema's. De ICO-Wizard maakt gebruik van deze thema-uitwerkingen vertaald naar inkooponderdelen, waarmee de voor aanbestedingen en inkopen noodzakelijke scherpte in de eisen verder wordt bereikt.

In de inkooponderdelen is nadere scherpte bovenop de BIO-eisen aangebracht m.b.v. andere marktstandaards zoals andere ISO-normenkaders (dan ISO27002), Standard of Good Practice, NIST, COBIT en BSI. Door deze inkooponderdelen te hanteren voor eisen aan aanbestedingen en inkopen, ontstaat een aanzienlijk completer en beter valideerbare veiligheidsvraag, dan wanneer alleen de BIO zou worden gebruikt.

De ICO-Wizard is gevuld met een compleet pakket van informatiebeveiligingseisen, behorende bij de inkooponderdelen Algemeen Ketenpartners, Huisvesting IV, Toegangsbeveiliging, Applicatieontwikkeling, Serverplatform, Clouddiensten, Communicatievoorzieningen, Procesautomatisering (CSIR), Softwarepakketten en de bestaande toepasselijke richtlijnen Secure Software Development (SSD), SSD Mobile, ICT-beveiligingsrichtlijnen voor webapplicaties van NCSC en de PToLU-lijst van het Forum voor Standaardisatie.

ICO-Wizard

Met de ICO-Wizard (www.BIO-overheid.nl/ICO) kunnen eisenpakketten worden geselecteerd die aansluiten op verschillende typen aan te besteden/in te kopen producten/diensten.
De gebruiker klikt de van toepassing zijnde inkooponderdelen aan en kan nog enkele extra selecties meegeven, waarmee eisen met bepaalde kenmerken (zoals product of proceseis) kunnen worden in- of uitgesloten. Naast de basisselectie op de inkooponderdelen, biedt de ICO-Wizard de mogelijkheid aanvullende eisen te selecteren bij de gekozen inkooponderdelen. Zo kan men de

gekozen inkooponderdelen nog completeren men aanvullende privacy-eisen, laten tonen welke BIO-Overheidsmaatregelen van toepassing zijn bij de gekozen inkooponderdelen en voor hoog-risico situaties ook aanvullingen met ABDO-eisen selecteren.

De aanvullende privacy-eisen zijn o.m. gebaseerd op de 7 Privacy-by-Design-principes, de privacy baseline en de ISO27701 en zijn nuttig als privacy en rol speelt in de aanbesteding.

De BIO-Overheidsmaatregelen zijn verplicht voor overheidsorganisaties. Ze zijn weliswaar verwerkt in het standaardeisenpakket maar het kan soms nuttig zijn ze expliciet te tonen.

De **ABDO**-eisen (Algemene Beveiligingseisen voor Defensieopdrachten) kunnen worden ingezet als er sprake is van een hoger dreigingsniveau. De ABDO richt zich op statelijke actoren, waarvoor ook BIO-BBN3 was beoogd.
De ABDO hanteert daarbij het begrip 'Te Beschermen Belang' (TBB) en maakt onderscheid op 4 niveaus van bescherming van specifieke informatie en fysieke objecten: TBB-4 Departementaal Vertrouwelijk, TBB-3 Confidentieel, TBB-2 Geheim en TBB-1 Zeer Geheim. In de ICO-wizard kunnen deze niveaus apart en in combinatie geselecteerd worden en toegevoegd worden aan het basiseisenpakket.

Risicoanalyse in de ICO-Wizard

De informatiebeveiliging (IB) maatregelen die een organisatie treft buiten de in de BIO voorgeschreven maatregelen, zijn afhankelijk van de te mitigeren risico's. Het werken met de BIO veronderstelt dan ook het maken van risicoafwegingen/risicoanalyses. De eisen die aan leveranciers worden gesteld, moeten worden beschouwd in het licht van deze risicoafwegingen.

De ICO-Wizard is erop gericht de opdrachtgever en het inkoopteam te ondersteunen bij het stellen van de juiste informatiebeveiligingseisen. Aan het voorgestelde eisenpakket kan echter worden toe- of afgedaan o.b.v. de risico-afwegingen. De wizard helpt hierbij door per geselecteerde eis de risico's te tonen die (mede) door de desbetreffende eis gemitigeerd kunnen worden.

Feitelijk is dit een opt-out aanpak: de eisen gelden, tenzij je ze o.b.v. risicoafweging wijzigt/laat vallen. Het voordeel van het tonen van de gemitigeerde risico's is dat de actoren in het inkoopproces – ook als ze vooraf geen risicoanalyse hebben uitgevoerd - toch worden geconfronteerd met de potentiele risico's die uitnodigen tot een bewuste keuze.

De gehanteerde risico's steunen op de tabel standaarddreigingen van open source tool voor risicoanalyse RAVIB en zijn aangevuld met specifieke risico's uit gehanteerd brondocumenten.

Selectie en Exportmogelijkheden

De ICO-Wizard presenteert, na invullen van de webapplicatie, op het scherm het geselecteerde eisenpakket. Het resultaat van de gemaakte selectie op het scherm toont per eis een korte beschrijving, een verwijzing naar de uitgebreide beschrijving in het bron-document en suggesties voor de verificatiemethode.

Door selecties te maken die passen bij de karakteristiek van de in te kopen producten en diensten wordt op deze wijze een set van eisen verkregen die met de aanbesteding meegestuurd kan worden (de *Word-export*) naar de inschrijvers/leveranciers. Als de opdrachtgever vanuit risicoafweging geen wijzigingen aangeeft, dan kunnen deze eisen als uitgangspunt gelden voor de aanbesteding, contracten, acceptatie en levering van het product/de dienst.

Naast de Word-export kun je gebruiken maken van de *Excel-export*. Dit document geeft naast de gegevens in de Word-export aanvullende informatie. Met name de relatie van de beveiligingseisen met de risico's die ze helpen mitigeren zijn hierin terug te vinden. Daarnaast zijn werkkolommen opgenomen voor het vastleggen van de uitvraag van de eisen en (RFC) criteria bij de beoordeling van inschrijvingen op de aanbesteding.