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 software producten 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.

ICO-Wizard

Met de ICO-Wizard 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 prioriteit, product-proceseis) kunnen worden in- of uitgesloten.

De Wizard presenteert op het scherm het geselecteerde eisenpakket, dat vervolgens ook als compleet en opgemaakt Word-document kan worden gedownload.

Het resultaat van de gemaakte selectie op het scherm en in het Word-document toont per eis onder meer 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 standaardeisen verkregen die met de aanbesteding meegestuurd kunnen 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.

Risicoanalyse in de ICO-Wizard

De 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. Ook de eisen die aan leveranciers worden gesteld zullen moeten worden beschouwd in het licht van deze risicoafwegingen.

De ICO-Wizard is erop gericht de opdrachtgever/budgethouder en het inkoopteam te ondersteunen bij het stellen van de juiste beveiligingseisen. 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 worden gemitigeerd. 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 door hun zichtbaarheid uitnodigen tot een bewuste keuze.

De gehanteerde risico's steunen op de tabel standaarddreigingen van open source tool voor risicoanalyse RAVIB.

Het fundament van de Wizard

De eisen in de Wizard zijn gebaseerd op een stevig fundament dat is ontleend aan de markstandaard ISO27002. De BIO is daarvan direct afgeleid en vormt op zijn beurt weer de basis voor een aantal nadere uitwerkingen naar samenhangende thema's. De ICO-Wizard maakt gebruik van deze thema-uitwerkingen, waarmee de voor aanbestedingen en inkopen noodzakelijke scherpte in de eisen wordt bereikt. Doordat de thema's ruwweg kunnen worden gezien als inkooponderdelen, kunnen bij in te kopen producten-diensten passende eisenpakketten worden samengesteld.

In de thema-uitwerkingen is nadere scherpte aangebracht en zijn blinde vlekken ingevuld m.b.v. andere marktstandaards zoals andere ISO-normenkaders (bijv. bij Cloud), Standard of Good Practice, NIST, COBIT en BSI. De opzet van de thema-uitwerkingen is uniform door het gebruik van de methode SIVA (de letters staan voor: Structuur, Inhoud, Vorm en Analysevolgorde). Deze methodiek maakt het mogelijk sluitende normenkaders te ontwikkelen en biedt een eenvormige syntax voor de beschrijving van de normen. Lees bij NORA-online meer over de SIVA-methode.

De SIVA-methodiek is ontwikkeld door Wiekram N.B. Tewarie PhD. aan de Vrije Universiteit.

Door de genoemde thema-uitwerkingen 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 nu gevuld met de eisen, behorende bij de inkoopsegmenten

- Huisvesting IV,
- Toegangsbeveiliging,
- Applicatieontwikkeling,
- Serverplatform,
- Communicatievoorzieningen,
- Clouddiensten

En is verder aangevuld met bestaande toepasselijke richtlijnen Secure Software Development (SSD), SSD Mobile, ICT-beveiligingsrichtlijnen voor webapplicaties van NCSC en de PToLU-lijst van het Forum voor Standaardisatie.