Beveiligingsmaatregelen BIO UMw Portaal

Benodigde maatregelen op basis van de BIO

Inhoudsopgave

1. Inleiding

Er is een risicoanalyse uitgevoerd voor het gebruik van het Uitwisselingsmechanisme werk Portaal, kortweg UMw Portaal. Op basis van deze risicoanalyse gelden er specifieke maatregelen vanuit de Baseline Informatiebeveiliging Overheid (BIO) voor het UMw Portaal en de gebruikers.
In de BIO is beschreven dat voor informatiesystemen binnen de overheid basisbeveiligingsniveau 2 (BBN2) het uitgangspunt vormt. BBN2 is van toepassing als:

- er vertrouwelijke informatie wordt verwerkt;
- mogelijke incidenten leiden tot bestuurlijke commotie;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

In het kader van privacy is daarnaast ook het niveau van beveiliging vastgesteld voor het UMw Portaal. Aan de hand van de DPIA komen de volgende maatregelen naar voren. Aangezien het UMw Portaal een open source component betreft, moet de DPIA nogmaals worden doorlopen voor de eigen organisatie. Hiervoor is de DPIA van VNG beschikbaar ter inspiratie. Deze is te vinden op Gitlab, onder documentatie: BBN2.

Het UMw Portaal voldoet op technisch vlak en op het gebied van privacy aan BBN2, maar er zijn nog enkele maatregelen waar organisaties zelf mee aan de slag moeten. Voordat het UMw Portaal op het platform van gemeenten kan draaien en gemeenten aan de slag kunnen met het UMw Portaal, moeten IT en andere relevante verantwoordelijken (denk aan: proceseigenaren, functioneel beheerders, lijnmanagers en dienstenleverancier) zorgen dat er deze maatregelen zijn ingevoerd.

Hieronder volgt een overzicht van de praktische uitwerking van maatregelen die van toepassing zijn op gemeenten en hun medewerkers die het UMw Portaal gaan gebruiken. Het maatregelnummer is gerelateerd aan het maatregelnummer uit de BIO. Meer informatie over de BIO en de bijpassende maatregels en controls vindt u op de website van IBD.

2. Maatregelen

2.1. Beheer en bedrijfsmiddelen

Informatieclassificatie

Maatregel uit BIO: 8.2.3.1
De informatie die binnen het UMw Portaal gebruikt wordt is geclassificeerd als BBN2. Dit betekent dat de gegevens binnen het UMw Portaal slechts toegankelijk mogen zijn voor de functionarissen die daarvoor zijn aangesteld en bevoegd zijn. Hierdoor wordt informatie beschermd tegen onbevoegde openbaarmaking of misbruik. Gemeenten gebruiken en verwerken voor meerdere bedrijfsprocessen nu ook al informatie die geclassificeerd is als BBN2. De toegang en het gebruik van de middelen en de gegevens binnen het UMw Portaal moet op dezelfde wijze geregeld te zijn.

Aandachtsgebieden hiervoor zijn:
- Veilige toegang tot werkstations van de gemeente.
- Authenticatie en autorisatie van de gebruikers van het UMw Portaal.
- Regels voor het gebruik van de informatie en middelen.

Betrokken rollen:
- Proceseigenaar
- ICT
- (C)ISO/ Informatiebeveiligingsfunctionaris

2.2. Toegangsbeveiliging

Beheer van toegangsrechten van gebruikers

Maatregel uit BIO: 9.2.2.1
Gezien het feit dat het UMw Portaal BBN2 informatie bevat, is de toegang hiertoe en het gebruik ervan beperkt tot enkel een aantal bevoegde personen. De bevoegde functionaris (meestal proceseigenaar of management) moet toegang verlenen aan de bevoegde personen. De bevoegde functionaris moet hier ook een procedure voor inrichten of een bestaande procedure aanvullen.

Maatregel uit BIO: 9.2.2.2
Bij het gebruik van het UMw Portaal is functiescheiding niet van toepassing. Wel is het belangrijk dat de medewerkers die gebruik gaan maken van het UMw Portaal de juiste autorisaties krijgen, afhankelijk van hun rol. Deze autorisaties worden toegekend door de bevoegde functionaris. Dit heeft een afhankelijkheid met maatregel 9.2.2.1 en het is aan te raden om deze taken binnen hetzelfde proces op te nemen.

Maatregel uit BIO: 9.2.4.1
Om te zorgen dat alleen bevoegde gebruikers toegang krijgen tot gegevens in het systeem moet er een proces komen om gebruikersnamen en wachtwoorden op een veilige, controleerbare manier bij de gebruikers te krijgen. Gemeenten gebruiken op dit moment ook andere BBN2 informatie, waarbij een dergelijk proces al noodzakelijk is. Dit is bij de meeste gemeenten daarom ook al ingericht en moet ook gebruikt worden voor het UMw Portaal. Het verstrekken van de gebruikersgegevens is eenvoudig in dit bestaande proces te integreren.

Maatregel uit BIO: 9.2.5.2
Het kan voorkomen dat tijdens de halfjaarlijkse controle op de toegangsrechten en autorisaties blijkt dat er gebruikers zijn die onterecht toegang hebben tot het systeem. Dat kan mogelijk een inbreuk zijn op de bescherming van de gegevens. Een dergelijke situatie moet ook als zodanig behandeld worden door de proceseigenaar. Registreer de afwijking en onderzoek of er wellicht misbruik is gemaakt van de onterechte toegang.

Maatregel uit BIO: 9.2.5.3
Om te zorgen dat het UMw Portaal aan de beveiligingsmaatregelen van BBN2 voldoet en blijft voldoen, moet de proceseigenaar de uitgegeven toegangsrechten van gebruikers minimaal eenmaal per half jaar beoordelen. Als gebruikers de toegangsrechten en autorisaties niet meer nodig hebben, moeten die op dat moment direct ingetrokken worden door de proceseigenaar. Dit geldt ook voor de andere processen met BBN2 informatie. Probeer deze taken ook in de bestaande processen te integreren.

2.3. Beveiliging bedrijfsvoering

Bedieningsprocedures en verantwoordelijkheden

Maatregel uit BIO: 12.1.1.1
De bevoegde gebruikers moeten weten hoe ze met het UMw Portaal werken. Daarvoor moet een handleiding beschikbaar zijn. Deze handleiding beschrijft hoe men met het systeem werkt en daarnaast ook hoe men met de BBN2 informatie binnen het systeem om hoort te gaan. Ook moet er een handleiding zijn voor de ICT-beheerders waarin het correcte beheer van het UMw Portaal is beschreven.

Als basis hiervoor is de VNG gebruikers- en beheerdershandleiding te gebruiken, deze staan op de website van de VNG.

Overwegingen betreffende audits van informatiesystemen

Maatregel uit BIO: 12.7.1.1

Het kan voorkomen dat er een audit plaats moet vinden op het systeem en de informatie die daarin verwerkt wordt. Audits moeten de productie zo min mogelijk verstoren. Een audit zal dus altijd in afstemming met en na goedkeuring van de proceseigenaar plaatsvinden. Bij de afstemming wordt het tijdstip en de specifieke toegang tot systemen en data, noodzakelijk voor de audit, besproken.

2.4. Communicatiebeveiliging

Informatietransport

Maatregel uit BIO: 13.2.2.2

Het UMw Portaal werkt met BBN2 informatie. De proceseigenaar is verantwoordelijk voor de bescherming van de gegevens. Ook bij het eventueel optreden van incidenten, bijvoorbeeld bij ongeautoriseerde toegang tot de gegevens, is de proceseigenaar verantwoordelijk. Dergelijke incidenten moeten altijd gemeld en opgevolgd worden. Het melden van informatiebeveiligingsincidenten moet geïntegreerd worden met het bestaande incidentmanagementproces, voor zover dat nog niet is ingeregeld. Op deze manier kunnen alle betrokkenen een informatiebeveiligingsincident melden.

3. Meer informatie

Meer informatie over de maatregelen van de BIO vindt u op de website van de IBD.

Alle andere informatie over het UMw Portaal is terug te vinden op:

- De website van VNG
- Gitlab (techniek)