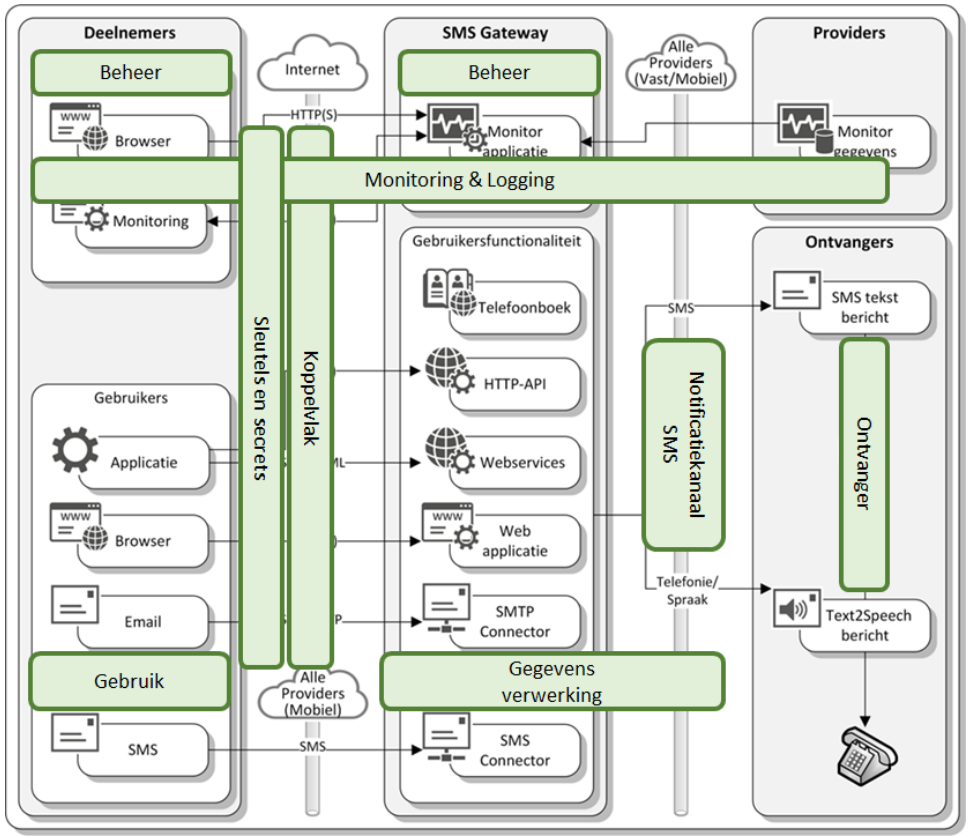
Bijlage E SMS-Gateway en maatregelen

In deze Bijlage wordt een toelichting gegeven op de maatregelen die getroffen dienen te worden op de SMS-Gateway in het kader van risico's van Nationale vsecurity-by-designeiligheid van bepaalde Deelnemers. De toelichting wordt gegeven aan de hand van onderstaand figuur.



Figuur 1 SMS-Gateway en de gevraagde maatregelen

Toelichting

Gebruik

Bij het gebruik van de SMS-Gateway dient er een strikte scheiding te zijn tussen de Deelnemers, zodat het niet mogelijk is dat gebruikers van de ene Deelnemer de gegevens van andere Deelnemers kunnen inzien of de gegevensverwerking kunnen beïnvloeden.

Beheer (Deelnemers)

Het beheer uitgevoerd door een Deelnemer dient inzage te hebben in de volledige Monitoring & Logging van die Deelnemer van de SMS-Gateway. Bovendien dient het gebruik en de verschillende technische mogelijkheden daartoe gecontroleerd te kunnen worden. De Deelnemer zal hiervoor de cryptografische sleutels en secrets beheren.

Sleutels en secrets

De cryptografische sleutels en secrets die nodig zijn voor de operationalisering en het beheer van de SMS-Gateway blijven onder verantwoordelijkheid en beheer van de Deelnemer en de Deelnemer heeft te allen tijde toegang tot deze sleutels en secrets conform vastgestelde procedures. Deze procedures worden vastgelegd in een cryptografisch sleutelmanagement protocol. Het kan nodig zijn dat bepaalde sleutels en secrets in een HSM[1] of TPM[2]-chip worden opgeslagen. Voor noodtoegang worden aanvullende procedures opgesteld.

Koppelvlak

Het koppelvlak tussen de Deelnemer en de SMS-Gateway verloopt via een besloten overheidsnetwerk zoals Diginetwerk, RON, etc. Ook voor alle beheerwerkzaamheden dient gebruik gemaakt te worden van een besloten overheidsnetwerk.

[1] Hardware Security Module
[2] Trusted Platform Module

Beheer (SMS-Gateway)

Het beheer door de Opdrachtnemer van de SMS-Gateway dient aangesloten te zijn op de Monitoring & Logging van de hele dienstverlening. Dit generieke beheer moet controleerbaar zijn voor alle Deelnemers.

Monitoring & Logging

De Monitoring & Logging geeft aan elke Deelnemer de volledige inzage op de werking van de SMS-Gateway (Gebruik, Beheer en Gegevensverwerking) voor de Deelnemer specifieke zaken en voor generieke beheerzaken (bijv. onderhoud op de infrastructuur). Deze Monitoring & Logging is aantoonbaar compleet en ongewijzigd en is gescheiden per Deelnemer. Verder is deze aangesloten op het Security Operations Centre van de Deelnemer. Afwijkingen in de Monitoring & Logging worden als incident behandeld conform het incidentenproces van de Deelnemer.

Gegevensverwerking

Bij de gegevensverwerking van de SMS-Gateway, dient er een strikte scheiding te zijn tussen de Deelnemers, zodat het niet mogelijk is dat gebruikers van de ene Deelnemer de gegevens van andere Deelnemers kunnen inzien of de gegevensverwerking kunnen beïnvloeden. Voor bepaalde Deelnemers is het noodzakelijk dat het telefoonnummer van de ontvanger en/of de inhoud van het bericht afgeschermd wordt van de Opdrachtnemer van de SMS-Gateway.

De gegevensverwerking dient per Deelnemer afgesplitst te kunnen worden en voortgezet te kunnen worden op een aangewezen infrastructuur en/of datacenterlocatie, waarbij gebruik gemaakt kan worden van alternatieve componenten voor het leveren van de dienst. Er wordt hiervoor in overleg met de Deelnemer een uitwijkplan opgesteld en geoefend. Bij een crisis van Nationale veiligheid[3] kan de Deelnemer de uitvoering van het uitwijkplan vereisen. De crisis-organisatie kan bij uitwijk buiten de Deelnemer komen te liggen, en de werklocatie(s) en het in te zetten personeel kan aan extra beveiligingsmaatregelen onderworpen worden.

[3] Een en ander conform de Nationale Crisisstructuur, zie https://www.nctv.nl/onderwerpen/n/nationale-crisisstructuur

Notificatiekanaal (SMS)

Het notificatiekanaal is zodanig ingericht dat de SMS-Gateway een directe netwerkkoppeling met Nederlandse telecomproviders heeft. Voor buitenlandse telecomproviders mag een andere route genomen worden. Voor bepaalde Deelnemers is het noodzakelijk dat het bericht direct afgeleverd wordt bij de betreffende Nederlandse telecomprovider[4]. Voor bepaalde Deelnemers is het noodzakelijk dat het gebruikte telefoonnummer van de ontvanger direct na aflevering verwijderd wordt uit de administratie van de SMS-Gateway.

Er zijn in de techniek waarborgen dat het juiste (en ongewijzigde) bericht bij de juiste telecomprovider wordt afgeleverd. De vertrouwelijkheid van de berichten is niet van dien aard dat deze end-to-end versleuteld moeten worden, maar het gebruik van technieken als Rich Communication Services (RCS) zijn wel wenselijk.

Ontvanger

De ontvanger van het bericht moet kunnen controleren dat het bericht daadwerkelijk afkomstig is van de Deelnemer. De ontvanger krijgt geen inzage in de (interne) gegevensverwerking van de SMS-Gateway of de aanlevering van het bericht bij de SMS-Gateway.

Controle van de maatregelen

Er wordt door de Opdrachtnemer een (Informatie)Beveiligingsfunctionaris aangewezen voor de opdracht. Deze Beveiligingsfunctionaris is de primaire contactpersoon voor de aanvullende contracteisen Risk, Compliance en Informatieveiligheid. De functionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert jaarlijks een Zelfinspectie uit op basis van de BIO[5] en de ABRO[6]. De resultaten van de Zelfinspectie en de opvolging van bevindingen zijn schriftelijk vastgelegd en maken deel uit van de Assurance van de opdracht.

[4] En dus niet via een andere telecomprovider
[5] Baseline Informatiebeveiliging Overheid
[6] Algemene Beveiligingseisen Rijksoverheid Opdrachten