

Bijlage 7: Visie op informatiebeveiliging

Een belangrijke ambitie van HbR omvat haar functie als 's werelds slimste én veiligste haven'. Deze ambitie geldt zowel binnen het fysieke als binnen het digitale domein. Daarnaast is een deel van HbR momenteel door de Nederlandse overheid aangewezen als Aanbieder Essentiële Diensten en in die hoedanigheid geclassificeerd als Vitaal B. De beschikbaarheid, integriteit en vertrouwelijkheid van ondersteunende systemen zijn dan ook van essentieel belang. Het Havenbedrijf Rotterdam is daarin terughoudend in het nemen van risico's.

Robuustheid en veiligheid zijn hierbij vanzelfsprekend van groot belang. HbR zoekt een Opdrachtnemer die deze doelstelling onderstreept. Een partij die dit zowel in woord én gedrag ondersteunt en die bijdraagt in de realisatie van de ambitie van HbR. Gezien de vitale rol van HbR worden hoge eisen gesteld aan security en compliancy. Om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens in de toekomst te garanderen en verder te borgen laat HbR haar systemen periodiek (penetratie-)testen en auditen volgens marktconforme standaarden.

De integrale inrichting van informatiebeveiliging binnen Havenbedrijf vindt risico gebaseerd plaats, waarin maatregelen genomen op basis van een uitgevoerde risicoanalyse. Daarbij is de proportionaliteit van de (kosten van) maatregelen in vergelijking tot de waarde van informatie(systemen) een belangrijke afweging.

Verwachtingen

Om de hierboven visie te bereiken verwacht HbR ten aanzien van informatiebeveiliging het volgende:

Proactieve informatiebeveiliging

Van Opdrachtnemer wordt verwacht dat hij volledig transparant is ten aanzien van de beveiligingsstatus en -updates van alle componenten. De geleverde diensten zijn altijd up-to-date en security-incidenten en andere externe dreigingen worden vroegtijdig ontdekt, gemeld en proactief met passende maatregelen beantwoord. Opdrachtnemer werkt op basis van risico gebaseerde informatiebeveiliging, waarin kwetsbaarheden worden geclassificeerd conform CVSS 3.0.

Dat betekent dat zowel de oplossing als de diensten van Opdrachtnemer continu voldoen aan het geldende HbR Informatiebeveiligingsbeleid en het HbR Informatiebeveiligingsplan. Opdrachtnemer is bekend met, handelt volgens en beweegt nadrukkelijk mee met actuele en toekomstige wetgeving met betrekking tot informatiebeveiliging en privacy gedurende looptijd van het contract. Denk hierbij concreet aan geldende AVG-richtlijnen maar vooral ook toekomstige WBNi2 (NIS2) wetgeving geldend voor o.a. vitale infrastructuur en managed serviceproviders.

Ten aanzien van informatiebeveiliging is Opdrachtnemer verantwoordelijk voor het totaalpakket aan aangeboden dienstverlening. Hierbij is Opdrachtnemer enerzijds zelf verantwoordelijk voor de inrichting, het doorvoeren en de borging van informatiebeveiliging op applicatie- en systeemniveau op het gebied van o.a. authenticatie, autorisatie, interface en eventueel maatwerk code.

Opdrachtnemer is tevens verantwoordelijk voor het aanpakken van hiaten binnen informatiebeveiliging van haar dienstverlening en in het proactief doen van voorstellen tot en het uitvoeren van het doorvoeren van mitigerende acties en beheersmaatregelen.