Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Informatiebeveiliging van meldkamers

Een onderzoek naar het vormgeven van risicomanagement

Plan van aanpak

Inhoudsopgave

1 Inleiding

1.1 Aanleiding voor het onderzoek

De meldkamers voor politie, brandweer, ambulance en marechaussee zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting kan leiden en een bedreiging vormt voor de nationale veiligheid. De meldkamers zijn daarom onderdeel van de Nederlandse vitale infrastructuur[1].

De meldkamers zijn knooppunten voor informatie en communicatie in nood- en crisissituaties. Voor wie in nood verkeert, is de meldkamer het eerste contact met de hulpdiensten van de brandweer, ambulance, politie en de marechaussee. Voor hulpverleners is een meldkamer de plek vanwaar zij informatie ontvangen over een incident en waar zij om ondersteuning kunnen vragen. Meldkamers zijn ook cruciaal bij de rampenbestrijding en crisisbeheersing en worden ingezet bij het bewaken van de openbare orde en opsporing.

Een verstoring van de informatie en communicatie kan de uitvoeringstaken van de meldkamers ernstig in gevaar brengen. Cybercriminaliteit vormt op dit moment een toenemende bedreiging voor de vitale infrastructuur[2], en daarmee voor de informatie- en communicatiesystemen van de meldkamers.

Vanaf 1 januari 2020 beheert de Nationale Politie de meldkamers. Zij moet zorgen voor de opbouw van een netwerk van operationeel en technisch geschakelde meldkamers onder een centraal beheer. Van de politie mogen wij daarmee verwachten dat zij de informatie- en communicatiesystemen van de geschakelde meldkamers afdoende beveiligt tegen verstoring.

De Inspectie JenV wil onderzoeken of in het afgelopen jaar de basis is gelegd voor een passend informatiebeleid, zoals bedoeld in de informatiebeveiligingsrichtlijnen die voor overheidsinstellingen gelden.

[1] *Cybersecuritybeeld Nederland 2020*, Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020)
[2] Idem

1.2 Context

Voldoende weerbaar zijn

Cybercriminaliteit is een lucratief crimineel businessmodel geworden. Dat is zorgelijk, want vrijwel alle overheidsprocessen en diensten zijn in hoge mate afhankelijk van ICT. Met het verstoren van systemen van overheden, ontneem je burgers de toegang tot belangrijke overheidsinformatie en hun persoonlijke gegevens of zelfs tot noodhulp.

De Inspectie JenV houdt toezicht op de vitale infrastructuur van de meldkamers. Zij let daarbij op de vorming van een visie op informatiebeveiliging en de uitwerking daarvan in een passend beleidsplan. De toepassing van deze plannen bepaalt uiteindelijk of de meldkamers bij cyberdreigingen voldoende weerbaar zijn.

Informatiebeveiliging van de meldkamers

In 2020 werd de *Wijzigingswet meldkamers* van kracht. De wet bepaalt dat de meldkamers gaan samenwerken en elkaars taken kunnen overnemen. De minister van JenV belegde het beheer van de meldkamers bij de Nationale Politie die daarvoor een speciaal organisatieonderdeel vormde: de Landelijke meldkamersamenwerking, de LMS. De directeur van dit verband is als de Chief Information Officer eindverantwoordelijk voor het beheer van informatie van de meldkamers, waaronder de zorg voor de informatie- en communicatiesystemen en de beveiliging van deze informatie.

Risicomanagement als basisvoorwaarde voor informatiebeveiliging

Van de LMS wordt verwacht dat zij de informatie van de meldkamers beveiligt tegen verstoring en uitval zoals bedoeld in het *Voorschrift informatiebeveiliging rijksdienst*, de standaarden ISO 27001 en ISO 27002 en de daarop gebaseerde *Baseline informatiebeveiliging overheid*. Deze richtlijnen beschrijven het basisniveau waaraan iedere overheidspartij minimaal moet voldoen, en geeft de uitgangspunten voor de procesmatige inrichting van de informatiebeveiliging[3]. Dit is voor iedere overheidsorganisatie anders en is daarmee maatwerk.

De richtlijnen beschrijven het inrichten en toepassen van risicomanagement als de basisvoorwaarde voor het functioneren van een goed beveiligingsbeleid. Dit komt erop neer dat een overheidsorganisatie procesmatig risicobeperkende maatregelen treft op basis van de evaluatie van haar bedrijfsmiddelen. Daarnaast dat zij de vastgestelde risico's analyseert. ISO 27001 en 27002 verwijzen voor het inrichten en toepassen van risicomanagement naar de uitgangspunten in ISO 27005. Dit impliceert daarmee het toepassen van ISO 27005, als de standaard voor risicomanagement.

[3] NEN-ISO/IEC 27001 moet worden toegepast op het inrichtingen en toepassen van een managementsysteem voor informatiebeveiliging. NEN-ISO/IEC 27002 moet worden toegepast op het formuleren van beheersmaatregelen inzake informatiebeveiliging. De verplichting geldt op basis van pas toe, leg uit. Zie: www.forumstandardisatie.nl

2 Onderzoek

2.1 Doelstelling van het onderzoek

De Inspectie JenV wil met dit onderzoek bereiken dat de meldkamers voldoende weerbaar zijn tegen cyberincidenten. Hiervoor is het nodig om uit te zoeken hoe het risicomanagement is ingericht en wordt toegepast. Daarmee worden eventuele leemtes in de opzet van de informatiebeveiliging inzichtelijk en bespreekbaar gemaakt. De Inspectie JenV wil op deze wijze bijdragen aan het waarborgen van de informatieveiligheid van de meldkamerfunctie.

2.2 Centrale vraag en onderzoeksvragen

Met dit onderzoek wil de Inspectie JenV een antwoord geven op de volgende centrale vraag:

Hoe is het risicomanagement op de informatiebeveiliging van de meldkamers vormgegeven?

Om tot een antwoord te komen op deze vraag, beantwoordt de Inspectie de volgende onderzoeksvragen:

- Hoe heeft de LMS het risicomanagement van de meldkamers ingericht en geborgd?
- Hoe zijn de risico's voor de veiligheid van de informatie geïdentificeerd?
- Hoe zijn vervolgens de risico's voor de veiligheid van de informatie geanalyseerd en geëvalueerd?
- Hoe zijn de maatregelen voor risicobeperking gekozen en vastgesteld?
- In welke mate zijn de overblijvende risico's geaccepteerd?

2.3 Afbakening

Dit onderzoek beschrijft de inrichting en de toepassing van de informatiebeveiliging van de meldkamers. Hierbij wordt nagegaan of de informatiebeveiliging daadwerkelijk is gebaseerd op risicomanagement, zoals bedoeld in het *Voorschrift informatiebeveiliging rijksdienst*, de *Baseline informatiebeveiliging overheid* en ISO 27005.

Van deze ISO-standaard hanteert de Inspectie enkel de uitgangspunten uit de hoofdstukken 7, 8, 9 en 10 die specifiek gaan over de opzet en toepassing van risicomanagement. De onderzoeksvragen zijn hierop afgestemd. De tabel in de bijlage van dit plan geeft een overzicht van deze selectie. De andere onderdelen van ISO 27005 zoals monitoring, review, communicatie en consultatie, zijn geen onderdeel van risicomanagement en blijven daarmee buiten beschouwing.

Het onderzoek vindt plaats bij de LMS en de informatiebeveiligingsorganisatie van de Nationale Politie (IBO). Ook spreken wij met het directoraat-generaal Politie en Veiligheidsregio's van het ministerie van JenV. Dit is omdat bij de LMS de beheerverantwoordelijkheid ligt voor de informatiebeveiliging. Deze ligt niet bij de afzonderlijke meldkamers. De IBO is de uitvoerder van de informatiebeveiliging van de meldkamers. Vanuit het directoraat-generaal Politie en Veiligheidsregio's loopt een programma dat tot doel heeft het realiseren van de kwalitatieve verbeteringen in het meldkamerdomein.

2.4 Onderzoeksaanpak

Het beschrijven van het risicomanagement en het vaststellen van mogelijke leemtes in de opzet van de informatiebeveiliging, vraagt om een stapsgewijze aanpak. Deze paragraaf zet uiteen welke stappen worden gezet om tot een antwoord te komen op de centrale vraag: Hoe is het risicomanagement op de informatiebeveiliging van de meldkamers vormgegeven?

Stap 1: Informatiebeveiliging van de meldkamers

De eerste stap richt zich op de informatiebeveiliging vanuit het perspectief van de meldkamers.

In gesprekken met de directeur/CIO van de LMS, de functionaris voor informatiebeveiliging en andere medewerkers nemen de inspecteurs kennis van de visie op informatiebeveiliging. Ook het verloop van het traject voor de inrichting van de informatiebeveiliging en de totstandkoming van het samenwerkingsverband van meldkamers komt daarbij aan de orde. Daarnaast wordt besproken welke partijen een rol spelen in de informatiebeveiliging hoe de verantwoordelijkheden zijn belegd. Ook spreekt de Inspectie met het directoraat-generaal Politie en Veiligheid over informatiebeveiliging en het programma voor kwalitatieve verbeteringen in het meldkamerdomein.

Stap 2: Inrichting en borging van het risicomanagement

In de tweede stap onderzoekt de Inspectie welke maatregelen de LMS treft om de meldkamers weerbaar te maken tegen cyberincidenten. De Inspectie wil hiervoor van de LMS weten hoe het risicomanagement voor de meldkamers is ingericht en geborgd, zoals bedoeld in ISO 27005.

De feitelijke inrichting en borging van het risicomanagement stelt de Inspectie vast aan de hand van documenten die zij opvraagt bij de LMS en de IBO. De uitkomsten worden aansluitend besproken in de interviews die de Inspectie houdt met de CIO en medewerkers van de LMS, en met de information securitymanager en medewerkers van de IBO, de uitvoerder van de informatiebeveiliging van de meldkamers.

In de gesprekken komt aan de orde: hoe de risico's voor de veiligheid van de informatie zijn geïdentificeerd; en hoe vervolgens de risico's voor de veiligheid van de informatie zijn geanalyseerd en geëvalueerd. Daarnaast wil de Inspectie van de LMS weten hoe de maatregelen voor risicobeperking zijn gekozen en vastgesteld; en in welke mate de overblijvende risico's zijn geaccepteerd. De details van deze thema's en de bijbehorende aandachtspunten staan beschreven in de bijlage.

Stap 3: Het groepsgesprek

De bevindingen uit de voorgaande stappen legt de Inspectie in een bijeenkomst terug aan de LMS om te peilen in hoeverre de bevindingen in algemene zin herkend worden.

In het gesprek beschrijft de Inspectie haar voorlopige bevindingen over het vormgeven van het risicomanagement op de informatiebeveiliging van de meldkamers. Dit gebeurt in relatie tot de uitgangspunten van ISO 27005. De Inspectie benoemt in het gesprek eventueel geconstateerde leemtes in de inrichting en borging van het risicomanagement en vraagt de LMS om hierop te reageren. De uitkomsten van deze drie stappen worden verwerkt in een rapportage aan de minister van JenV.

2.5 Samenhang met andere onderzoeken

Dit onderzoek richt zich specifiek op het beleid voor informatiebeveiliging. De Inspectie deed eerder onderzoeken naar de meldkamers. Het verschil is dat deze onderzoeken gingen over continuïteit in het afhandelen van noodmeldingen.

In 2015 verscheen het rapport *Meldkamers* van de Inspectie Justitie en Veiligheid en het Agentschap Telecom, en in 2019 het vervolgrapport *Continuïteit van meldkamers*. Uit het onderzoek bleek dat de regionale meldkamers die moeten reageren op 112-noodoproepen zeer kwetsbaar zijn voor verstoring van de taakuitvoering. Zij hebben te weinig personeel en hebben niet de mogelijkheid om elkaars taken volledig over te nemen als zij door een calamiteit worden getroffen. Het afhandelen van noodmeldingen kan daardoor vertraging oplopen.

In 2020 presenteerden de Inspectie Justitie en Veiligheid en het Agentschap Telecom en de inspectie Gezondheidszorg en Jeugd het gezamenlijk rapport *Onbereikbaarheid van 112 op 24 juni 2019*. Het rapport beschrijft het handelen van de overheid, KPN, hulpdiensten en zorgorganisaties bij de onbereikbaarheid van het alarmnummer 112 in 2019. Zij waren onvoldoende voorbereid op de totale onbereikbaarheid.

2.6 Communicatie

De Inspectie JenV informeert de directeur van de Landelijke meldkamer-samenwerking per brief over het voorgenomen onderzoek en het plan van aanpak. De korpschef van de Nationale Politie, en de directeur-generaal Politie van het ministerie JenV ontvangen hiervan een afschrift. Het plan van aanpak wordt gepubliceerd op de website van de Inspectie.

De te interviewen functionarissen krijgen vooraf het interviewprotocol toegestuurd. De gespreksverslagen worden na het interview in het kader van wederhoor aan de

participanten voorgelegd. Het conceptrapport wordt voor wederhoor voorgelegd aan de directeur van de Landelijke meldkamersamenwerking.

Na verwerking van eventuele wederhoor en de vaststelling van het rapport, biedt de Inspectie het rapport aan de minister van JenV aan. De directeur van de Landelijke meldkamersamenwerking, de korpschef van de Nationale politie en de directeur-generaal Politie van het ministerie JenV ontvangen hiervan een afschrift. De Inspectie publiceert het rapport op haar website, met uitzondering van details die door openbaarmaking de vitale taakuitvoering van de meldkamers kan schaden.

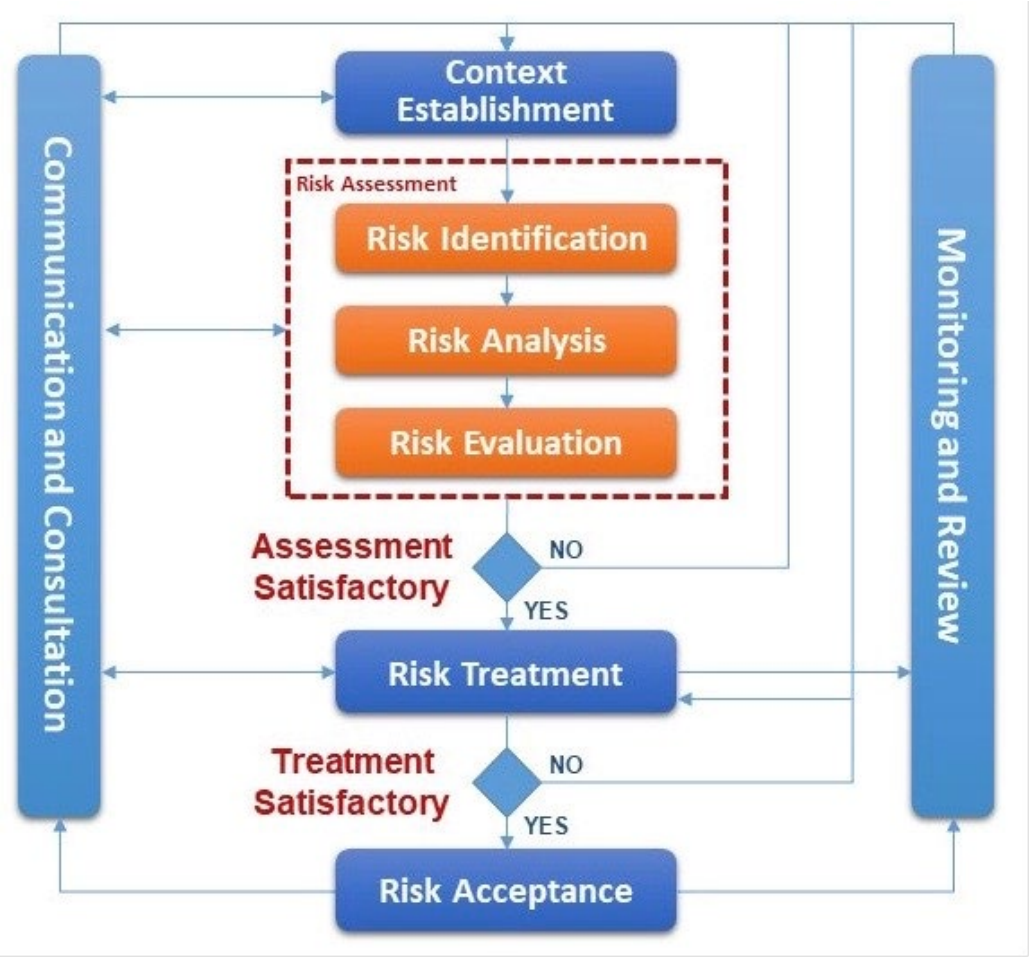
Bijlage: Aandachtspunten in het onderzoek

Risicomanagement volgens ISO 27005

De standaard ISO 27005 beschrijft de wijze waarop een organisatie grip kan krijgen op risico's die verband houden met het gebruik van informatie bij het uitvoeren van haar taken. Het inrichten van een managementsysteem voor informatiebeveiliging staat daarbij centraal. Dit managementsysteem is gebaseerd op de Deming-kwaliteitscirkel. Deze cirkel bestaat uit vier fases: plan, do, check en act. De planfase bevat de activiteiten gerelateerd aan het identificeren en analyseren van de risico's. De standaard geeft echter geen specifieke methode voor het inrichten van het risicomanagement proces zelf. ISO 27005 biedt de standaardrichtlijnen voor het inrichten van informatie risicomanagement. De standaard geeft daarbij vooral invulling aan de eisen die ISO 27001 stelt aan dit proces. Het werkt de genoemde planfase uit in de volgende handelingen:

- Het bepalen van de reikwijdte, context en criteria voor het risicomanagement (context establishment)
- Het beoordelen van de risico's (risk assessment)
- Het treffen van risicobeperkende maatregelen (risk treatment)
- en het accepten van de rest-risico's (risk acceptance).

Daarnaast zijn er nog de twee activiteiten voor monitoren en evalueren en communiceren, die we in dit onderzoek buiten beschouwing laten.



Afbeelding: Weergave van de uitgangspunten voor het procesgericht beheer van risico's in de informatiebeveiliging volgens ISO 27005.

Het bepalen van de reikwijdte, context en criteria voor het risicomanagement is het feitelijke opzetten van het raamwerk voor risicomanagement. De beoordeling van risico's is onderverdeeld in drie deelactiviteiten: risico-identificatie, risicoanalyse en risico-evaluatie.

Het eerste onderdeel, risico-identificatie, gaat over het in kaart brengen van de relevante risico's. De omvang van de geïdentificeerde risico's worden vervolgens tijdens de tweede stap, de risicoanalyse, geschat. De derde stap richt zich op het vergelijken van de omvang van de geïdentificeerde risico's met de van tevoren bepaalde risico criteria. Tijdens deze stap wordt bepaald of het risico acceptabel is. Als het risico niet acceptabel is, zal in de volgende activiteit van risicobehandeling bepaald gaan worden op welke wijze het risico zal worden afgehandeld. Voorbeelden van afhandeling zijn daarbij het risico mijden, het risico overdragen of maatregelen nemen om de omvang van het risico te verkleinen. Bij de laatste stap wordt vastgelegd welke overblijvende risico's worden aanvaard.

Aandachtspunten in het onderzoek	***Leidraad voor het beschrijven van de bestaande situatie***	***Referentie aan ISO 27005***
Reikwijdte, context en criteria (context establishment)		
Het bepalen van de context	De organisatie bepaalt de externe en interne context voor het beheren van informatie risico's. Hiervoor stelt zij de basiscriteria op, definieert de reikwijdte en de grenzen en organiseert het uitvoeren van informatierisicomanagement.	7.1
Het inrichten en toepassen van informatie risicomanagement	De organisatie beschrijft hoe zij het proces van risicomanagement heeft ingericht en toepast. Hierin zijn criteria opgenomen voor risico evaluatie, criteria voor impact en criteria voor risico acceptatie. (zoals bedoeld in 7.2.2, 7.2.3 en 7.2.4)	7.2.1
Het bepalen van criteria voor risico-evaluatie	De organisatie definieert criteria voor het evalueren van risico's.	7.2.2
Het bepalen van criteria voor gevolgen	De organisatie definieert criteria voor het bepalen van de gevolgen van incidenten.	7.2.3
Het bepalen van criteria voor acceptatie van risico's	De organisatie definieert criteria voor het accepteren van risico's.	7.2.4
Het bepalen van de reikwijdte van het informatie risicomanagement	De omgeving waarin de organisatie haar taken uitvoert, is geanalyseerd en beschreven. De organisatie brengt alle relevante bedrijfsprocessen en bedrijfsmiddelen in kaart. De uitkomsten van de omgevingsanalyse en de relevante bedrijfsprocessen en bedrijfsmiddelen zijn in de risicobeoordeling meegenomen.	7.3
Het vastleggen van de verantwoordelijkheden en de uitvoeren van informatie risicomanagement	De organisatie legt de verantwoordelijkheden en de uitvoering van informatie risicomanagement vast. De wijze van uitvoering van het informatie risicomanagement is vastgelegd.	7.4
Risicobeoordeling (risk assessment)		
Het beoordelen van de risico's	De organisatie identificeert de risico's, beschrijft deze en prioriteert deze ten opzichte van de risico- evaluatie criteria en de doelstellingen die relevant zijn voor de organisatie.	8.1
Het identificeren van de bedrijfsmiddelen (assets)	De organisatie identificeert de bedrijfsmiddelen die relevant zijn voor de reikwijdte van de risicobeoordeling.	8.2.2
Het identificeren van dreigingen	De organisatie identificeert de relevante dreigingen en de bronnen voor deze dreigingen.	8.2.3

Het identificeren van de bestaande maatregelen	De organisatie identificeert de relevante bestaande en geplande maatregelen.	8.2.4
Het identificeren van de kwetsbaarheden	De organisatie identificeert de kwetsbaarheden die geëxploiteerd kunnen worden door de geïdentificeerde dreigingen en de kunnen leiden tot schade aan de geïdentificeerde bedrijfsmiddelen.	8.2.5
Het identificeren van de gevolgen	De organisatie identificeert de gevolgen van het aantasten van de beschikbaarheid, integriteit en de vertrouwelijkheid van haar bedrijfsmiddelen /informatie.	8.2.6
Het bepalen van de gevolgen	De organisatie bepaalt de gevolgen voor haar bedrijfsvoering van een mogelijk of daadwerkelijk beveiligingsincident. Zij houdt daarbij rekening met de gevolgen van het doorbreken van haar informatiebeveiliging zoals het aantasten van de beschikbaarheid, integriteit en vertrouwelijkheid van haar bedrijfsmiddelen.	8.3.2
Het bepalen van de kansen op een incident	De organisatie bepaalt de kans op optreden van de incidenten.	8.3.3
Het bepalen van het risiconiveau	De organisatie bepaalt het risico voor elk van de relevante incidenten.	8.3.4
Het evalueren van de risico's	De organisatie vergelijkt de risico's met de criteria voor het evalueren en accepteren van risico's.	8.4
Risicobehandeling (risk treatment)	De organisatie kiest maatregelen voor risicobeperking en stekt dit vast.	9
Risico-acceptatie (risk acceptance)	De organisatie beschrijft aan de hand van de risicocriteria welke rest risico's de organisatie aanvaardt. De directie heeft goedkeuring verleend aan de overblijvende risico's.	10

Missie Inspectie Justitie en Veiligheid

De Inspectie Justitie en Veiligheid houdt voor de samenleving, de ondertoezichtgestelden en de politiek en bestuurlijk verantwoordelijken
toezicht op het terrein van justitie en veiligheid
om inzicht te geven in de kwaliteit van de taakuitvoering en de naleving van regels en normen,
om risico's te signaleren
en om organisaties aan te zetten tot verbetering.
Hiermee draagt de Inspectie bij aan een rechtvaardige en veilige samenleving.

Dit is een uitgave van:
Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag
Contactformulier | www.rijksoverheid.nl/jenv

December 2020