Ministerie van Defensie

Toezichtjaarverslag 2022
Beveiligingsautoriteit

Colofon

Beveiligingsautoriteit

Adres
Kalvermarkt 32
Postbus 20701
2511 CB ‘s-Gravenhage

Postadres
2500 ES ’s-Gravenhage
MPC 58B

Opsteller
Dhr. M. van Ree MIM
Toezichthouder integrale beveiliging

Datum
Maart 2023

Inhoudsopgave

Voorwoord

Het Ministerie van Defensie levert een belangrijke bijdrage aan de bevordering van vrede en veiligheid in de wereld. Personeel, informatie en materieel zijn van wezenlijk belang om de taken van de defensieorganisatie effectief uit te voeren. De organisatie moet bij de taakuitvoering onder alle omstandigheden kunnen vertrouwen op de continuïteit en betrouwbaarheid van de bedrijfsprocessen en de benodigde mensen en middelen. Die betrouwbaarheid garandeert de organisatie onder meer door beveiligingsmaatregelen te treffen, zoals het beveiligen van de door de defensieonderdelen aangemerkte Te Beschermen Belangen (TBB). Dit kan zowel informatie zijn in fysieke- of elektronische vorm, als IT-diensten, fysieke locaties en materieel. De ernst en omvang van potentiële schade bepaalt de mate van de vereiste beveiliging. Onder 'schade' valt zowel materiële schade als immateriële schade. Beveiliging wordt uitgevoerd op basis van risicomanagement. Hierdoor is er een balans tussen het vereiste niveau van beveiliging en de consequenties van de beveiligingsmaatregelen voor de uitvoering van de bedrijfsprocessen, de voor beveiliging beschikbare middelen en de eventueel realistisch geaccepteerde restrisico's.

Dit toezichtjaarverslag 2022 Beveiligingsautoriteit (BA) geeft inzicht in de uitvoering van toezicht en de hoofdlijnen van de resultaten daarvan van de BA op de integrale beveiliging. Daarbij geldt het toezichtjaarplan als uitgangspunt, aangevuld met inzichten die de BA heeft opgedaan in de rol van toezichthouder.

Integrale beveiliging (*security*) is niet hetzelfde als bedrijfsveiligheid (*safety*). Bedrijfsveiligheid omvat onder andere bedrijfshulpverlening, brandweerzorg, vliegveiligheid, arbeidsomstandigheden en de toepassing van milieuregels.

Doelstelling

De doelstelling van het Defensie Beveiligingsbeleid (DBB) is het waarborgen van de continuïteit en betrouwbaarheid van de bedrijfsprocessen, zodat het Ministerie van Defensie zijn taken ongestoord en onder alle omstandigheden kan uitoefenen.

De Beveiligingsautoriteit,

voor deze,
het afdelingshoofd Beveiliging, Gegevensbescherming en Documentaire Informatievoorziening

Kolonel H.J. Schuthof, MSc, EMSD, MA

1 Toezicht 2022

1.1 Inleiding

Het Toezichtjaarplan Beveiligingsautoriteit 2022[1] vormt de basis van het uitgevoerde toezicht. Naast de meeste vaste toezichtonderwerpen, kwamen in 2022 ook specifiek geselecteerde toezichtonderwerpen aan bod. Door de beperkte capaciteit van de BA zijn de overgebleven toezichtonderwerpen echter opgenomen in het toezichtjaarplan Beveiligingsautoriteit 2023.

In 2023 wordt het aantal functies binnen de BA uitgebreid, waardoor de toezichtcapaciteit toeneemt. Het toezichtjaar 2022 van de BA kenmerkt zich vooral door normatief toezicht, verdere ontwikkeling van het normenkader ten behoeve van systeemgericht toezicht, ad-hoc toezicht, toezicht in het kader van accreditaties en samenwerkingen. De BA vervult bij het houden van toezicht verschillende rollen. Naast interne toezichthouder heeft de BA ook de rol van *Program Security Officer* in relatie tot het *Special Access Program* horende bij de F-35 en de rol van *National Security Authority* voor het militaire domein (NSA-MoD).

1.2 Verbeteracties naar aanleiding van defensiebreed onderzoek

Defensiebreed onderzoek in 2021 wees uit dat de bezuinigingen en reorganisaties de afgelopen decennia afbreuk hebben gedaan aan de beveiliging van Defensie. Als gevolg van capaciteitsproblemen is de realisatie van verbeteracties vertraagd. Dit had invloed op de keuze van toezichtonderwerpen van de BA. De BA wil namelijk de toezichtdruk op de organisatie waar mogelijk minimaliseren. De BA volgt de voortgang van verbeteracties op de voet en participeert actief.

1.3 Samenwerking

De interne toezichthouders bij Defensie werken samen om de samenhang en de kwaliteit van toezicht te verbeteren. De interne toezichthouders zijn: de Beveiligingsautoriteit (BA), de Functionaris voor Gegevensbescherming (FG), de Inspectie Militaire Gezondheidszorg (IMG), de Inspectie Veiligheid Defensie (IVD), het Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS) en de Militaire Luchtvaart Autoriteit (MLA). Zij werken samen door onder andere de toezichtagenda's op elkaar af te stemmen en gezamenlijk het toezichtproces te versterken op het gebied van methodologie en redactie.

Toezichtberaad

In 2020 hebben de interne toezichthouders zich verenigd in het Toezichtberaad Defensie. De Inspecteur-Generaal der Krijgsmacht (IGK) en een vertegenwoordiger van het Bureau Secretaris-Generaal nemen als toehoorder deel aan het beraad. De IGK is geen toezichthouder, maar zijn onderzoeken verrijken wel het inzicht in de staat en het functioneren van de defensieorganisatie. De Inspecteur-Generaal Veiligheid is als coördinerend toezichthouder voorzitter van het beraad.

[1] Beveiligingsautoriteit. (2021). *Toezichtjaarplan 2022.*

2 Hoofdlijnen uit het toezicht

2.1 Introductie methoden van toezicht

Bij normatief toezicht kijkt de toezichthouder naar de effectiviteit van getroffen beveiligingsmaatregelen. Dat kan zowel integraal, als aan de hand van normen binnen een van de deelgebieden ('Algemeen', 'Personeel', 'Fysiek', 'Informatie' en 'Industrie'). Normatief toezicht is gericht op de TBB, maar ook op andere zaken zoals ruimtes en informatiesystemen. Met systeemgericht toezicht kijkt de BA naar de opzet, het bestaan en de effectieve werking van het managementsysteem, waarmee wordt gegarandeerd dat bij een defensieonderdeel aan het DBB wordt voldaan. Bij deze vorm van toezicht staat de mate van borging van de zogenaamde *Plan-Do-Check-Act*-cyclus (PDCA-cyclus) centraal.

2.2 Hoofdlijnen uit het toezicht

Accreditatiestatus kritieke informatiesystemen

In samenwerking met de beveiligingsketen houdt de BA voortdurend zicht op de voortgang van de accreditaties van de kritieke informatiesystemen. De BA concludeert dat de beveiligingsstatus slechts minimaal is verbeterd. In 2022 is de status van slechts één kritiek informatiesysteem omgezet van een 'tijdelijke goedkeuring' naar een 'volwaardige accreditatie'. Voor de overige nog af te ronden accreditaties geldt dat het uitvoeren van verbeterplannen langer duurt dan gewenst. De oorzaak is gerelateerd aan gewijzigde prioriteringen, schaarse capaciteit en wisselend eigenaarschap. Als gevolg hiervan ontbreekt het aan regie, monitoring en sturing. De BA dringt voor een aantal accreditaties aan op een betere sturing door de verantwoordelijke eigenaren van de desbetreffende informatiesystemen.

Aanbeveling 1
De toezichthouder adviseert de eigenaren van kritieke informatiesystemen de voortgang van verbeterplannen actief te monitoren en hier tijdig op te sturen.

Accreditatiestatus van locaties

De BA behandelt in zijn rol als Security Accreditation Authority (SAA) meerdere site-accreditatieverzoeken van locaties en/of compartimenten (voortaan: locaties) voor hoog gerubriceerde informatiesystemen. De BA heeft hiervoor een steekproef gehouden en de fysieke beveiligingsmaatregelen van een aantal locaties beoordeeld. De conclusie is dat voor deze locaties aanvullende beveiligingsmaatregelen noodzakelijk zijn, voordat het accreditatieproces voor deze locaties kan worden vervolgd en goedkeuring voor het gebruik ervan kan worden gegeven. De SAA heeft de eigenaar opgedragen een plan van aanpak te schrijven om de fysieke beveiliging van de locaties te borgen conform het DBB. Dit verzoek is vanwege onvoldoende voortgang door de BA geëscaleerd.

Tempest

Tempesteisen zijn eisen om te voorkomen dat informatie via straling lekt. Verworven producten waar tempesteisen op van toepassing zijn, bleken in de afgelopen jaren kwalitatief onvoldoende na levering. Inspanningen hebben in 2022 geleid tot een lichte kwaliteitsverbetering. De 100%-controle van tempestproducten blijft van kracht.

Elektronische Veiligheidsonderzoeken

Elektronische Veiligheidsonderzoeken (EVO) moeten uitsluiten dat ongeautoriseerd kan worden meegeluisterd met hoog gerubriceerde gesprekken in gerubriceerde ruimtes. De onderzoekscapaciteit bleek in de voorgaande toezichtjaren onvoldoende om aan de vraag te kunnen voldoen, maar is in 2022 uitgebreid. Omdat de capaciteit nog steeds onvoldoende is om aan de groeiende vraag te voldoen, is verdere uitbreiding noodzakelijk en ook voorzien in 2023.

Beveiligingsplannen

Elke locatie dient een actueel beveiligingsplan te hebben als onderdeel van het kwaliteitsmanagementsysteem en om risico's te beheersen. In een beveiligingsplan staat beschreven hoe de beveiliging van de locatie en de beveiliging van de aanwezige TBB is georganiseerd. Ook worden de beveiligingsrisico's beschreven, welke mitigerende beveiligingsmaatregelen zijn getroffen om risico's tot het minimum te beperken en welke restrisico's overblijven. De toezichthouder concludeerde na uitgevoerde steekproeven dat geen van de beoordeelde beveiligingsplannen actueel of compleet was. Daarnaast concludeerde toezichthouder dat het format beveiligingsplan in het DBB is opgenomen, maar dat het ontbreekt aan een eenduidige toepassingsnorm.

Aanbeveling 2
De toezichthouder draagt de organisatie op om actief aandacht te besteden aan de compleetheid en de actualiteit van beveiligingsplannen.

Aanbeveling 3
De toezichthouder adviseert de BA als beleidsmaker een eenduidige norm in het DBB op nemen voor het toepassen van het format beveiligingsplan.

Risicobeheersing

Afhankelijk van het classificatieniveau worden restrisico's aan de BA voorgelegd. De BA heeft mede hierdoor zicht op de geaccepteerde restrisico's van de hogere TBB en bewaakt deze. De toezichthouder gebruikt deze informatie bij het toezicht houden of bij het uitvoeren van steekproeven.

De toezichthouder concludeert dat een aantal onderkende restrisico's niet juist is beschreven in beveiligingsplannen en in een aantal gevallen ook niet aan de daartoe verantwoordelijke functionarissen is voorgelegd. Restrisico's op de juiste wijze documenteren en voorleggen aan de verantwoordelijke functionarissen is van essentieel belang om de organisatie in staat te stellen te kunnen sturen op deze restrisico's. Daarnaast merkt de toezichthouder op dat er grote verschillen zijn tussen het aantal gemelde restrisico's van de defensieonderdelen. Hier wordt geen waardeoordeel aan gehangen, maar de BA geeft hier in het komende toezichtjaar extra aandacht aan.

Aanbeveling 4
De toezichthouder draagt de organisatie op om risico's tot het minimum te beperken, deze op de juiste wijze te documenteren en eventuele restrisico's voor te leggen aan de daartoe verantwoordelijke functionarissen, deze te laten accorderen en vast te laten leggen.

Incidentbeheersing

De toezichthouder kan alle gemelde beveiligingsincidenten inzien en voert hier verschillende analyses op uit. In de afgelopen vijf jaar is het aantal verloren en gestolen defensiepassen enorm toegenomen. Ondanks dat verloren of gestolen defensiepassen uit toegangssystemen worden verwijderd, blijft het risico bestaan dat deze passen buiten Defensie in omloop raken.

Aanbeveling 5
De toezichthouder vraagt aandacht voor een verantwoordelijke omgang met defensiepassen. Bewustwordingsprogramma's kunnen helpen om het aantal gestolen of verloren defensiepassen te verminderen.

Kwaliteit beveiligingsketen

De functionele beveiligingsketen ondersteunt de commandant (hieronder worden onder andere ook de hoofd van dienst en de lijnmanager verstaan) bij zijn verantwoordelijkheid voor de integrale beveiliging. De beveiligingsketen bestaat uit een BA voor het ministerie, een Beveiligingscoördinator, meerdere beveiligingsfunctionarissen per defensieonderdeel en een Beveiligingscoördinator voor de Commandant der Strijdkrachten (CDS) en de Militaire Inlichtingen- en Veiligheidsdienst Defensie (MIVD).

De kwaliteit van de beveiligingsketen is lastig te meten, maar wordt bereikt door bijvoorbeeld opleidingen, betrokkenheid in processen en samenwerking, maar ook door een juiste belegging van de rol van beveiligingsfunctionaris. Deze taak is vaak een 'neventaak' van een medewerker. In veel gevallen is dezelfde medewerker ook belast met eenzelfde rol voor bijvoorbeeld veiligheid, milieu of huisvesting. Er is in toenemende mate aandacht voor beveiliging in het algemeen en soms voor beveiliging in specifieke situaties in het bijzonder. Door het beleggen van de rol van beveiligingsfunctionaris als 'neventaak' en de groeiende aandacht voor beveiliging, ontstaat een kwetsbaarheid en een *Single Point of Failure*.

Aanbeveling 6
De toezichthouder vraagt aandacht voor verbetering van de kwantiteit en kwaliteit van de ondersteuning voor beveiliging door beveiligingsfunctionarissen. Overweeg om bij eenheden met een substantiële integrale beveiligingscomponent een 'functie beveiligingsfunctionaris' in te stellen, in plaats van deze rol te beleggen als neventaak.

NATO-inspectie

Conform het NATO-beleid voerde de toezichthouder in de rol van NSA-MoD inspecties uit op de registratie van specifieke NATO-documentatie. De uitgevoerde inspecties zijn verwerkt in gerubriceerde toezichtrapporten met enkele aanbevelingen en aangeboden aan de betrokken commandant en de NATO.

Toezicht F-35-programma

In 2022 bezocht de BA in de rol van *Program Security Officer* (PSO) alle *Special Acces Program Facilities* (SAPF). Met het F-35-wapensysteem dient Defensie zich, naast het nationale beleid, te conformeren aan de richtlijnen van de Amerikaanse overheid. Deze richtlijnen zijn in het nationale beleid geïntegreerd. Alle programma-informatie van de F-35 krijgt de merking *Special Access Required*. Deze informatie wordt beveiligd conform te beschermen belang -categorie 1- en mag uitsluitend verwerkt worden in de hierboven genoemde SAPF-locaties. De uitgevoerde toezichtbezoeken zijn verwerkt in gerubriceerde toezichtrapporten en aangeboden aan de betrokken commandant.

Samenwerking met de FG

De BA hield samen met de FG en de verantwoordelijke van de afdeling Documentaire Informatievoorziening toezicht op de personeelsdossiers van Defensie die in beheer zijn gegeven aan het ABP/APG. Dit betrof een voortgangscontrole van het verbeterplan uit 2018. De resultaten zijn gedeeld met de desbetreffende verantwoordelijken.

Industrieveiligheid

Bedrijven belast met de uitvoering van gerubriceerde en/of vitale defensieopdrachten dienen te voldoen aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). Het Bureau Industrieveiligheid (BIV) van de MIVD houdt hier toezicht op in de rol van *Designated Security Authority* (DSA). De DSA-rol maakt onderdeel uit van de taak van de NSA-MoD. Toezicht bij de defensie-industrie is in 2022 op een beperkt deel van de ABDO-bedrijven in de portefeuille van BIV uitgevoerd en de prioriteitstelling naar aanleiding van beschikbare capaciteit ligt hieraan ten grondslag. In 2022 is toezicht gehouden op een aantal bedrijven. Hierbij zijn geen grote afwijkingen geconstateerd ten opzichte van de gestelde eisen.

3 Bijlage

Afkortingen

ABDO	Algemene Beveiligingseisen voor Defensieopdrachten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BA	Beveiligingsautoriteit
BIV	Bureau Industrieveiligheid
BNIVD	Beveiligingsnormen Inlichtingen- & Veiligheidsdiensten
DBB	Defensie Beveiligingsbeleid
DSA	Designated Security Authority
EU	Europese Unie
FG	Functionaris voor Gegevensbescherming
IGK	Inspecteur-Generaal der Krijgsmacht
IMG	Inspectie Militaire Gezondheidszorg
IVD	Inspectie Veiligheid Defensie
KMCGS	Korps Militaire Controleurs Gevaarlijke Stoffen
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MLA	Militaire Luchtvaart Autoriteit
NATO	North Atlantic Treaty Organization
NSA	National Security Authority
NSA-MoD	National Security Authority – Ministry of Defence
PDCA	Plan-Do-Check-Act
PSO	Program Security Officer
SAA	Security Accreditation Authority
SAPF	Special Access Program Facilities
SG	Secretaris-Generaal
TBB	Te Beschermen Belangen