Ministerie van Defensie

Toezichtjaarverslag 2021
Beveiligingsautoriteit

Colofon

Toezichthouder
Bestuursstaf (BS)
Directoraat-Generaal Beleid (DGB)
Directie Bedrijfsvoering en Evaluatie (DBE)
Beveiliging, Gegevensbescherming en Documentaire Informatievoorziening (BGD)
Beveiligingsautoriteit (BA)

Postadres
Kalvermarkt 32
Postbus 20701
2511 CB Den Haag

Opsteller
Dhr. M. van Ree MIM
Senior toezichthouder integrale beveiliging

Datum
Maart 2022

Inhoudsopgave

Voorwoord

Het toezichtjaarverslag BA 2021 geeft inzicht in de uitvoering en resultaten van het door de Beveiligingsautoriteit (BA) uitgevoerde toezicht op de integrale beveiliging van Defensie in 2021. Daarbij geldt het toezichtjaarplan als uitgangspunt, aangevuld met inzichten die de BA opdoet in haar regievoerende taak bij de uitvoering van het Defensie Beveiligingsbeleid (DBB).

Onderzoek heeft uitgewezen dat de bezuinigingen en reorganisaties over een periode van decennia, afbreuk hebben gedaan aan de beveiliging van Defensie. Aan deze conclusie worden oplossingen verbonden op korte- en lange termijn die de BA nauwlettend zal volgen.

Het toezichtjaarverslag bestaat uit vier delen. Het eerste deel beschrijft belangrijkste constateringen en de meest positieve ontwikkelingen. Vervolgens wordt in het tweede deel inzicht gegeven in de gehanteerde toezichtmethodiek. Daarna komen de paragrafen met de belangrijkste resultaten aan bod, samen met de constateringen uit het uitgevoerde toezicht in 2021 en het resultaat van samenwerkingen met andere toezichthouders.

De Beveiligingsautoriteit,

Voor deze,
Het afdelingshoofd Beveiliging, Gegevensbescherming en Documentaire Informatievoorziening
Kolonel H.J. Schuthof, MSc, EMSD, MA

1 Toezicht BA in 2021

Integrale beveiliging is een brede en systematische benadering van beveiliging, gericht op de continuïteit en betrouwbaarheid van de bedrijfsprocessen, zodat het Ministerie van Defensie haar taken ongestoord en onder alle omstandigheden kan blijven uitoefenen. De beveiligingsnormen zijn vastgelegd in het Defensie Beveiligingsbeleid en worden uitgevoerd op basis van risico-management en een kosten/batenanalyse met een samenhangend stelsel effectieve en efficiënte beveiligingsmaatregelen. De verantwoordelijkheid voor beveiliging is binnen Defensie belegd in de lijn. Deze verantwoordelijkheid betekent dat de verantwoordelijke commandanten de Te Beschermen Belangen (TBB) van Defensie moeten beveiligen conform het Defensie Beveiligingsbeleid.

Binnen het Ministerie van Defensie is de Beveiligingsautoriteit (BA) belast met het toezicht op de integrale beveiliging. De Aanwijzing SG A/948 over Toezicht bij Defensie is kaderstellend voor het toezicht op de implementatie en de naleving van het Defensie Beveiligingsbeleid. Jaarlijks stelt de BA een toezichtjaarplan en toezichtjaarverslag op. Het toezichtjaarplan en toezichtjaarverslag wordt in het Toezichtberaad besproken en door de SG vastgesteld.

1.1 Inleiding

De toezichtverantwoordelijkheid van de BA bestaat uit verschillende toezichtactiviteiten, die hieronder kort worden toegelicht.

Toezicht is outputgericht: bij toezicht beoordeelt de BA de effectiviteit van de getroffen beveiligingsmaatregelen en of daarmee wordt voldaan aan de DBB-normeringen. Deze vorm van toezicht wordt veelal op locatie uitgevoerd en/of in samenwerking met ter zake deskundigen in relatie tot NATO-, EU- en/of US-verplichtingen.

Toezicht ten behoeve van accreditaties: het accrediteren van een belang zoals bijvoorbeeld een fysiek te beschermen belang, ruimte of informatiesysteem, is een proces waarbij voorafgaand aan ingebruikname het bijbehorende beveiligingsplan wordt beoordeelt. Deze beoordeling kan integraal van aard zijn, of specifiek gericht zijn op een of meerdere deelgebieden binnen integrale beveiliging. De accrediterende instantie kan bepalen dat aanvullend fysiek toezicht wordt uitgevoerd voorafgaand aan of na de accreditatie.

Systeemgericht toezicht is procesgericht: bij systeemgericht toezicht kijkt de BA naar de inrichting van beveiligingsprocessen en beheersingsmaatregelen die noodzakelijk zijn voor een defensieonderdeel om aan het DBB te kunnen voldoen. Bij deze vorm van toezicht gaat het om de aanwezigheid, de opzet en de werking van een beveiligingsmanagementsysteem, en de mate waarin de Plan-Do-Check-Act cyclus (PDCA) is gewaarborgd. Dit is een cyclische methode met continue aandacht voor kwaliteitsverbeteringen.

Het toezichtjaarplan 2021 bevatte verschillende specifieke onderwerpen die tijdens het uitvoeren van toezicht worden meegenomen maar ook het monitoren van openstaande verbeterpunten uit de vorige toezichtjaren.

1.2 Deelgebied Fysiek & Personeel

De BA heeft in 2021 vanwege de coronapandemie slechts een beperkt aantal fysieke toezichtbezoeken uitgevoerd. Naast de fysieke toezichtbezoeken voor accreditaties zijn nog toezichtbezoeken uitgevoerd op verschillende locaties bij verschillende defensieonderdelen. Daarbij is de compleetheid en actualiteit van het beveiligingsplan integraal beoordeeld, samen met de effectiviteit van verschillende geïmplementeerde fysieke- en personele beveiligingsmaatregelen. De resultaten zijn in een gerubriceerd toezichtrapport aan de commandant en beveiligingcoördinator van de betreffende defensieonderdelen aangeboden. De bevindingen worden door de BA geregistreerd en gemonitord.

Toezicht F-35 programma
In 2020 heeft de Nederlandse Program Security Officer (PSO) vanuit de BA alle Special Access Program Facilities (SAP-F) bezocht in het kader van toezicht. Met het F-35 Air System dient Defensie zich, naast het nationale beleid, te conformeren aan richtlijnen van de Amerikaanse overheid. Deze richtlijnen zijn in het nationale beleid geïntegreerd. Daarom krijgt alle F-35 programma informatie de merking 'Special Access Required'. Deze informatie wordt op te beschermen belang -categorie 1- beveiligd en mag uitsluitend verwerkt worden in de hierboven genoemde SAP-F locaties. De uitgevoerde toezichtbezoeken zijn verwerkt in gerubriceerde toezichtrapporten en aangeboden aan de betreffende commandant. De bevindingen worden door de BA geregistreerd en gemonitord.

1.3 Deelgebied Informatiebeveiliging

Accreditatie kritieke systemen grotendeels op orde
De BA houdt voortdurend zicht op de voortgang van de accreditatie van de kritieke informatiesystemen en concludeert dat de beveiligingsstatus wederom is verbeterd. De meeste afgesproken verbeterplannen worden uitgevoerd, waardoor de eerder verleende tijdelijke goedkeuringen uiteindelijk kunnen worden omgezet in volwaardige goedkeuringen.

Beoordeling Algemene Rekenkamer (AR) over informatiebeveiliging
Op basis van een risico-inschatting heeft de Algemene Rekenkamer over 2021 geen eigen onderzoek gedaan bij het ministerie van Defensie voor het verantwoordingsonderzoek informatiebeveiliging. De Auditdienst Rijk (ADR) heeft wel onderzoek gedaan naar de opvolging van de AR aanbeveling. Op basis van een review van het werk van de ADR zal de AR besluiten of zij over de ontwikkelingen op informatiebeveiliging bij het ministerie van Defensie zullen rapporteren.

Beoordeling Audit dienst Rijk(ADR) over Centrale sturing op informatiebeveiliging
De ADR doet jaarlijks onderzoek naar de centrale sturing op de informatiebeveiliging getoetst op basis van een rijksbreed afgesproken volwassenheidsmodel. Voor dit jaar waren het de onderwerpen governance, risicomanagement en incidentmanagement. Op deze onderwerpen heeft Defensie een voor zichzelf passend ambitieniveau bepaald. Dit niveau heeft de ADR in 2021 opnieuw bevestigd.

Defensie Cyber Commando (DCC)
De BA heeft de locatie en een systeem van het DCC beoordeeld in het kader van een accreditatie. Voor het betreffende informatiesysteem en de locatie worden de aanbevelingen gevolgd, totdat deze zijn uitgevoerd. Op basis van de vastgestelde beveiligingsstatus is een voorlopige goedkeuring aan het systeem gegeven.

Toezicht in relatie tot accreditaties
De BA heeft naar aanleiding van accreditatie aanvragen, fysiek toezicht uitgevoerd op een aantal locaties. Daarbij is aan de hand van het accreditatiedossier en het beveiligingsplan van de locatie, de effectiviteit van de getroffen beveiligingsmaatregelen beoordeeld en het beveiligingsplan beoordeeld op compleetheid en actualiteit. Het toezichtrapport is aan de accrediterende instantie aangeboden. De bevindingen worden geregistreerd in een centraal bevindingenregister van de BA en de voortgang wordt gemonitord.

In samenwerking met de AIVD is toezicht uitgevoerd op een aantal AIVD-locaties. Deze locaties zijn voorzien van een goedkeuring.

1.4 Deelgebied industrieveiligheid

Bedrijven die gerubriceerde en/of vitale defensieopdrachten uitvoeren, 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).

Ook in 2021 waren de gevolgen van de coronapandemie merkbaar, waardoor ook dit jaar fysieke audits niet zijn uitgevoerd. Vanwege deze beperkingen is onderzocht op welke wijze het toezicht in een andere vorm door kan gaan. De focus van het toezicht lag op de lopende *compliance*-trajecten. *Compliance*-trajecten hebben als doel te komen op het vereiste beveiligingsniveau, door bevindingen uit een audit op te lossen. De toetsing is gedaan met een vernieuwde methodiek: de ‘In Control Verklaring’ (ICV), inclusief onderliggende bewijslast. Het BIV heeft deze nieuwe vorm van toezicht beproefd. De lessons learned hebben geleidt tot kleine procesaanpassingen, waardoor de kwaliteit van de methodiek omhoog is gegaan. In 2021 zijn er in totaal vijftien ICV-toetsingen in verschillende vormen uitgevoerd. Het resultaat is dat er elf *compliance*-trajecten zijn afgerond. De vier openstaande trajecten zijn door de BA tijdelijk goedgekeurd.

1.5 Systeemgericht toezicht

De afgelopen jaren hebben de defensieonderdelen en de BA de nodige stappen gezet om het toezicht te professionaliseren, zoals het intensiveren van toezicht door de defensieonderdelen zelf (eerstelijns toezicht). Ook heeft de BA meer systeemvragen (ter beoordeling van de opzet, het bestaan en de werking van het beveiligingsmanagementsysteem) opgenomen in het regulier toezicht. De BA gebruikt de bevindingen van de afgelopen jaren om bij alle defensieonderdelen systeemgericht toezicht uit te voeren. Daarbij kijkt zij naar de aanwezigheid van essentiële onderdelen van het benodigde integraal beveiligingsmanagement systeem (IBMS) en naar de beheersingsmaatregelen die een defensieonderdeel heeft geïmplementeerd om aan het DBB te voldoen.

Door de coronapandemie en de diverse maatregelen om het aantal contactmomenten te minimaliseren heeft de BA, net als in 2020, ook in 2021 besloten het systeemgericht toezicht vooral digitaal uit te voeren. De bestaande vragenlijst is aangepast en geeft per defensieonderdeel inzicht in de aanwezigheid, de opzet en de werking van een IBMS, of en hoe beveiligingsrisico's inzichtelijk zijn, of deze worden beheerst, en het volwassenheidsniveau per element binnen het IBMS.

De resultaten van systeemgericht toezicht komen nagenoeg overeen met de resultaten uit het toezichtjaar 2020. Dit houdt in dat elke defensieonderdeel beschikt over een IBMS en is voorzien van de noodzakelijke onderdelen. Omdat eerder het volwassenheidsniveau van het IBMS niet is gemeten, is het volwassenheidsniveau dit jaar toegevoegd aan de vragenlijst. Hierdoor is per onderdeel van het IBMS het door het defensieonderdeel zelf ingeschatte volwassenheidsniveau inzichtelijk gemaakt. Hieruit blijkt dat het bereikte volwassenheidsniveau door de defensieonderdelen voor de meeste onderdelen van het IBMS op niveau 3 wordt ingeschat. In onderstaande tabel zijn de verschillende niveaus weergegeven.

De BA als toezichthouder controleert deze inschattingen in de komende jaren en zal het ingeschatte niveau tevens gebruiken het minimale volwassenheidsniveau te bepalen en deze vast te leggen in de instructie rond toezicht als onderdeel van het DBB.

Level	Titel	Korte omschrijving
1	Initieel	Onbeheerst proces: niets digitaal of op papier aanwezig
2	Reactief	Procesbeheersing: procedures aanwezig, er wordt naar gewerkt, monitoring nog onvoldoende ingericht, Inrichting verschilt per dienstonderdeel
3	Berekend	Systeem: consistente processen over het defensieonderdeel, mensen en middelen op orde
4	Proactief	Borging: consistente processen over het defensieonderdeel, mensen en middelen op orde, monitoring ingericht
5	Optimaal	Continu verbeteren: werking beoordelingssysteem, beheerst omgaan met wijzigingen

1.6 Overig

Fysieke beveiligingstest
De BA heeft in samenwerking met de Rijksbeveiligingsambtenaar (RijksBVA) in 2021 een fysieke beveiligingstest laten uitvoeren. Deze test wordt uitgevoerd door een externe organisatie en heeft dit jaar plaatsgevonden op een locatie van de Koninklijke Marechaussee (KMar). Aan deze test zijn door de BA extra voorwaarden gesteld, namelijk dat de resultaten bruikbaar zijn voor de gehele defensieorganisatie, externe medewerkers tijdens het uitvoeren van de test geen risico lopen voor wat betreft gewapende interventies en dat geen onnodige escalaties binnen de KMar worden opgestart. Naar aanleiding van deze test zijn verbeteracties geïnitieerd op het gebied van beveiligingsbewustzijn.

Oefeningen / missies
De BA heeft in 2021 vanwege de coronapandemie geen toezicht uitgevoerd tijdens oefeningen en/of missies.

2 Beelden uit toezicht

2.1 Invloed coronapandemie

Door de coronapandemie en de diverse maatregelen om het aantal contactmomenten te minimaliseren heeft de BA, net als in 2020, ook in 2021 besloten om systeemgericht toezicht vooral digitaal uit te voeren. Tussen de twee periodes van coronamaatregelen heeft de BA een beperkt aantal fysieke toezichtbezoeken kunnen uitvoeren.

2.2 Algemeen

De uitgevoerde toezichtbezoeken, ongeacht de classificatie van het belang, leveren grotendeels negatieve resultaten op. Desondanks neemt de mate toe waarin Defensie controle heeft op de beveiliging. Toezichtbevindingen, voornaamste restrisico's en beveiligingsincidenten zijn centraal inzichtelijk, waardoor de organisatie beter in staat is om hierop te kunnen sturen. Dit heeft alles te maken met de ontwikkeling en professionalisering van beveiligingsmanagementsystemen en de verbetering van ketensamenwerking.

Verschillende dienstverleners binnen het beveiligingsdomein hebben in de afgelopen jaren problemen kenbaar gemaakt via managementrapportages en escalaties. Dit heeft geleid tot structurele verbeteringen op het vlak van ketensamenwerking, financiële middelen, capaciteit en kwaliteit van producten.

2.3 Ontwikkelingen binnen het domein

<u>Defensiebreed onderzoek</u>
Naar aanleiding van de toename van beveiligingsrisico's en gerelateerde meldingen, heeft de Directeur Directie Aansturen Operationele Gereedheid in opdracht van de Chef Defensiestaf in 2021 besloten een onderzoek uit te laten voeren. Het doel was inzicht verkrijgen in de aard en omvang van deze problematiek, de mate waarin deze problematiek defensiebreed is en mogelijke oplossingsrichtingen te definiëren langs de lijn van organisatorische-, bouwkundige- en elektronische maatregelen. Het onderzoek heeft uitgewezen dat de gemelde problematiek reëel is en defensiebreed speelt. Dit is het gevolg van decennia lang bezuinigen en reorganiseren met negatieve gevolgen voor het domein beveiliging. Omdat het een complex probleem is, vraagt het om een geïntegreerde aanpak (mensen, middelen, manieren en geld). Op basis van deze conclusie zijn in het onderzoek diverse aanbevelingen gedaan die begin 2022 nader zullen worden uitgewerkt. De BA zal deze ontwikkeling op de voet volgen en actief participeren.

Cyber Security.
Het *Cyber Security Beeld Nederland 2021*, mede opgesteld door de MIVD, geeft aan dat onverkort sprake is van bedreigingen van de digitale veiligheid door statelijke en niet-statelijke actoren. Deze digitale aanvallen kunnen vooralsnog worden afgeslagen door de bestaande beveiligings-maatregelen, zoals bijvoorbeeld firewalls en een goede wachtwoord-discipline. Dit neemt niet weg dat voor de bedreigingen van de toekomst, het steeds grotere belang van het Cyberdomein en de daaraan gerelateerde mogelijkheden en kwetsbaarheden in relatie tot informatie gestuurd optreden (IGO) een doorontwikkeling van nieuwe, proactieve en dynamische verdedigings-concepten noodzakelijk zal zijn.

Nieuwe impuls programma Grensverleggende IT
Defensie heeft een contract gesloten om de IT-infrastructuur de komende jaren volledig te vernieuwen met het programma Grensverleggende IT. Hiermee bouwt Defensie aan een nieuwe goed beveiligde en toekomstbestendige IT-voorziening. De BA monitort en begeleidt deze ontwikkelingen noodzakelijkerwijs intensief, zeker ook in relatie tot bovengenoemd evoluerend dreigingsbeeld.

Beschikbaarheid tempestproducten
Verworven producten waar tempesteisen (eisen om te voorkomen dat informatie via straling lekt) op van toepassing zijn, bleken kwalitatief onvoldoende, waardoor reparaties noodzakelijk waren. Hierdoor was er een tekort aan producten. Het afgelopen jaar is mede door een intensievere ketensamenwerking, deze problematiek opgepakt en is inmiddels de kwaliteit van de producten verbetert, waardoor de ontstane achterstanden kunnen worden weggewerkt.

Elektronische Veiligheidsonderzoeken nog steeds onvoldoende
Elektronische Veiligheidsonderzoeken worden ingezet om uit te sluiten dat ongeautoriseerd kan worden meegeluisterd met hoog gerubriceerde gesprekken in gerubriceerde ruimtes. De onderzoekscapaciteit bleek onvoldoende om aan de vraag te kunnen voldoen. De capaciteit wordt uitgebreid, waardoor dit zal verbeteren. Voor 2022 zullen nog wel prioriteiten moeten worden gesteld gezien het aantal te onderzoeken ruimtes.

Defensie Bewakings- en Beveiligingssysteem (DBBS) is vertraagd
Het project DBBS heeft nog steeds te kampen met vertragingen over de as van ontwikkeling, inrichting en goedkeuring van het systeem. Daardoor moeten bestaande en verouderde toegangs- en/of beveiligingssystemen in stand worden gehouden. De BA monitort de verdere voortgang.

Capaciteit DBBO verbeterd
De Defensie Bewakings- en Beveiligingsorganisatie (DBBO) bleek structureel onderbezet en heeft daarom verzocht om extra financiële middelen voor personele capaciteit. Voor de jaren 2022 en 2023 zijn additionele financiële middelen toegekend om dit te repareren.

Versterking samenhang en kwaliteit beveiligingsketen vordert
Binnen de gehele beveiligingsketen is onderkend dat de kennis en capaciteit in de loop der jaren achter is gebleven bij de ontwikkelingen. Om daar verbetering in te brengen is onder andere het DSO (Defensie Security Overleg) ingericht onder voorzitterschap van het Kenniscentrum Inlichtingen & Veiligheid. Het doel is innovatiever en toekomstgerichter te gaan werken om aan te sluiten bij de modernisering van de krijgsmacht conform de Defensievisie 2035. Wanneer daar beleids-consequenties uit voortvloeien, wordt gebruik gemaakt van bestaande processen.

Beschikbaarheid Nationale Crypto-producten
In de Defensievisie 2035 staat dat Defensie een technologisch hoogwaardig, informatie gestuurd en betrouwbare partner en beschermer wil zijn. Gezien de steeds groter wordende afhankelijkheid van IT is het cruciaal dat Defensie digitaal autonoom is en ook als zodanig kan blijven optreden. Een essentiële randvoorwaarde daarbij is het gebruik van hoogwaardige nationale crypto-producten. De vervanging van de huidige beschikbare producten is lopende, maar vergt wel de nodige additionele inspanningen van de BA en delen van JIVC. Defensie is daarnaast betrokken bij de Nationale Crypto Strategie (NCS) om als Rijk hiermee de nationale digitale soevereiniteit blijvend te kunnen borgen en zodoende beter voorbereid te zijn op de toekomst.

Cloud-ontwikkelingen
Voor de medische dienstverlening aan militairen wordt samenwerking met civiele partijen steeds belangrijker om de juiste medische ondersteuning te kunnen leveren en te blijven voldoen aan de wetgeving op dit terrein. Voor de vernieuwing van de IT-ondersteuning is gekozen voor het gebruik van civiele applicaties waardoor uitwisselbaarheid van gegevens wordt bevorderd, maar ook wordt voldaan aan de wetgeving. Deze applicaties worden door externe marktpartijen vanuit een externe Cloud aangeboden. In overleg met de Medische keten Defensie, de AVG-coördinator en Industrieveiligheid (ABDO) zijn passende beveiligingsmaatregelen afgesproken en geïmplementeerd met de betrokken marktpartijen.

2.4 Samenwerking Toezichthouders

De samenwerking van de BA met andere toezichthouders komt op verschillende manieren tot stand.

Beleidsmatig: in relatie tot de Algemene Verordening Gegevensbescherming (AVG), zijn binnen het DBB normen en maatregelen opgenomen om de verwerking van persoonsgegevens te herkennen en deze afdoende te beveiligen.

Procesmatig: de BA participeert actief binnen het toezichtberaad en heeft verschillende voorstellen gedaan in het belang van de samenwerking, zoals het bereiken van een eenduidige scoringsmethodiek voor systeemgericht toezicht, normen voor een managementsysteem, ontwikkeling van een begrippenkader voor centraal toezicht en een legitimatiebewijs voor de toezichthouders.

Uitvoerend: in 2021 zijn vanwege de coronapandemie geen gezamenlijke toezichtbezoeken uitgevoerd met andere toezichthouders. De geplande toezichtbezoeken zijn verplaatst naar de plannen voor het toezichtjaar 2022.