Ministerie van Defensie

Jaarverslag 2020
Beveiligingsautoriteit

ONGERUBRICEERD

Colofon

Bestuursstaf (BS)

Directoraat-Generaal Beleid (DGB)

Directie Bedrijfsvoering en Evaluatie (DBE)

Beveiliging, Gegevensbescherming en Documentaire Informatievoorziening (BGD)

Beveiligingsautoriteit (BA)

Kalvermarkt 32

Postbus 20701

2511 CB Den Haag

Opsteller:

M. van Ree

Inhoudsopgave

Voorwoord

Met integrale beveiliging wil Defensie vastgestelde te beschermen belangen beveiligen. Zij doet dit op basis van risicomanagement en een kosten/batenanalyse met een samenhangend stelsel effectieve en efficiënte beveiligingsmaatregelen. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de departementen: het lijnmanagement is daarmee integraal verantwoordelijk voor de beveiliging van de te beschermen belangen.

Het beveiligingsvoorschrift Rijksdienst 2013 bepaalt dat de Beveiligingsambtenaar van een departement (binnen Defensie is dit de Beveiligingsautoriteit (BA)) toezicht houdt op de integrale beveiliging van het departement, beveiligingsincidenten laat onderzoeken, hierover adviseert en toezicht houdt op de beveiligingsorganisatie van het departement. De Aanwijzing SG A948 Toezicht bij Defensie geeft de BA aanwijzingen voor het uitvoeren van toezicht op de implementatie van de defensiebrede kaders op het gebied van integrale beveiliging. Ter voorbereiding op de uitvoering van deze toezichttaak wordt jaarlijks een toezichtjaarplan BA opgesteld. Dit wordt in het toezichthoudersoverleg besproken en door de Secretaris-Generaal (SG) vastgesteld.

Het voorliggende toezichtjaarverslag BA 2020 geeft inzicht in de uitvoering en resultaten van het door de BA uitgevoerde toezicht op de integrale beveiliging in 2020. Daarbij geldt het toezichtjaarplan als uitgangspunt, aangevuld met inzichten die de BA opdoet in haar regie-voerende taak bij de uitvoering van het Defensie Beveiligingsbeleid (DBB).

De bevindingen uit dit toezichtjaarverslag worden besproken in het toezichtberaad met de overige toezichthouders binnen Defensie voordat het jaarverslag wordt aangeboden aan de SG. De frequentie van het toezichtberaad is in 2020 verhoogd; de toezichthouders komen nu tweemaandelijks bij elkaar onder leiding van de Inspecteur-Generaal Veiligheid (IGV). Zij hebben zich ten doel gesteld nauwer te gaan samenwerken om de kwaliteit, de samenhang en de effectiviteit van het toezicht te versterken. Daartoe worden toezichtjaarplannen op elkaar afgestemd om de effectiviteit van het interne toezicht te verbeteren en de toezichtlast te verlagen. Ook werken de toezichthouders meer samen om de methodologische en redactionele kwaliteit van het toezicht te verhogen en het systeemgerichte toezicht bij Defensie te versterken.

Het verslag 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. Gevolgd in het derde deel door de paragrafen met de belangrijkste resultaten, constateringen naar aanleiding van het uitgevoerde toezicht in 2020, en tot slot het resultaat van samenwerking met andere toezichthouders.

Hendrik J Schuthof
Digitally signed by Hendrik J Schuthof
Date: 2021.03.15 16:08:54 +01'00'

De Beveiligingsautoriteit,

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

1 Belangrijkste bevindingen Beveiligingsautoriteit

1.1 Systeemgericht toezicht nog in ontwikkeling

Bij systeemgericht toezicht wordt de aanwezigheid, de opzet en de werking van een securitymanagementsysteem bij de Defensieonderdelen beoordeeld. Een securitymanagementsysteem is een set van samenhangende methodes, beleid, procedures, werkinstructies om het DBB binnen een Defensieonderdeel uit te dragen, uit te voeren, te handhaven en te controleren. Het maakt het dus mogelijk het DBB binnen een defensieonderdeel te managen. Bij de inrichting van het systeem vormt het DBB het kaderstellende uitgangspunt en moet de Plan-Do-Check-Act (PDCA)-cyclus zijn gewaarborgd.

Het verkregen inzicht is nog onvoldoende om een kwalitatief oordeel te geven over de verschillende securitymanagementsystemen maar toont wel grote verschillen tussen de defensieonderdelen. Het DBB bevat geen normen waar een securitymanagementsysteem minimaal aan moet voldoen. Dat maakt het beoordelen of het toetsen van een security managementsysteem lastig. In 2021 zal dan ook een DBB instructie “Toezicht” worden opgesteld die vervolgens als toetsingskader zal dienen.

1.2 Fysieke beveiliging kwetsbaar

Er zijn binnen het deelgebied fysieke beveiliging een aantal zorgen/aandachtpunten die zijn te relateren aan interne en externe dienstverleners waar de organisatie afhankelijk van is om te komen tot positieve beveiligingsrendementen. De onderliggende problematiek is complex en het bereiken van oplossingen is een kwestie van de lange adem.

1.3 Informatiebeveiliging naar tevredenheid

De informatiebeveiliging van kritieke informatiesystemen die binnen Defensie zijn onderkend, is in control. Hoewel de accreditatiestatus van de kritieke informatiesystemen ten opzichte van 2019 gelijk is gebleven, vorderen de plannen ter verbetering. Ook verloopt binnen het IT-domein de samenwerking tussen de BA, Joint IV Commando (JIVC) en de Chief Information Officer (CIO) intensief en constructief, niet alleen voor de accreditatie van de kritieke systemen maar ook bij ad-hoc vraagstukken en beveiligingsincidenten. Nu ook de aanbesteding van “Grensverleggende IT” (GrIT) eind 2020 is voltooid, zal Defensie bouwen aan een nieuwe veilige en toekomstbestendige IT-infrastructuur waarbij de hierboven genoemde samenwerking cruciaal is.

1.4 Industrieveiligheid verbetert

De audits die Bureau Industrie Veiligheid (BIV) in opdracht van de BA uitvoerde waren gerelateerd aan accreditaties en her-audits. De resultaten van deze audits waren overwegend positief. De audits van de afgelopen jaren dragen bij aan een hoger integraal beveiligingsniveau bij de bedrijven.

1.5 Positieve ontwikkelingen

Ondanks thuiswerken niet méér gemelde beveiligingsincidenten in relatie tot thuiswerken

In 2020 is vanwege de COVID-19 situatie het thuiswerken een begrip geworden. Niet eerder werd op deze schaal gebruik gemaakt van de middelen die de organisatie verstrekt om thuis te kunnen werken. Positief is dat het vele thuiswerken in 2020 niet heeft geleid tot een merkbare groei van gemelde beveiligingsincidenten.

Steeds meer samenwerking binnen de beveiligingsketen

Naar aanleiding van beveiligingsincidenten in 2017 is in opdracht van de BA een centraal bezoekersregistratiesysteem ontwikkeld. Dit systeem is sinds 2020 in gebruik en heeft geleid tot defensiebrede verbeteringen zoals een uniform aanmeldproces, uniforme begeleiding en toezicht op bezoekers. Ook is een VoG op basis van een defensieprofiel ingevoerd.
Daarnaast is in 2020 de Basisadministratie Risicoplaatsen en Te beschermen belangen opgeleverd. Met dit systeem is er defensiebreed inzage in alle te beschermen belangen van de organisatie, is er een eenduidig beheerconcept en is het eenvoudiger om informatie tussen verschillende partijen en dienstverleners uit te wisselen. Beide systemen zijn ontwikkeld in nauwe samenwerking met de defensieonderdelen. Ze zijn ondersteunend aan zowel centrale als decentrale kritische beveiligingsprocessen.

Oprichting Securitykennisforum

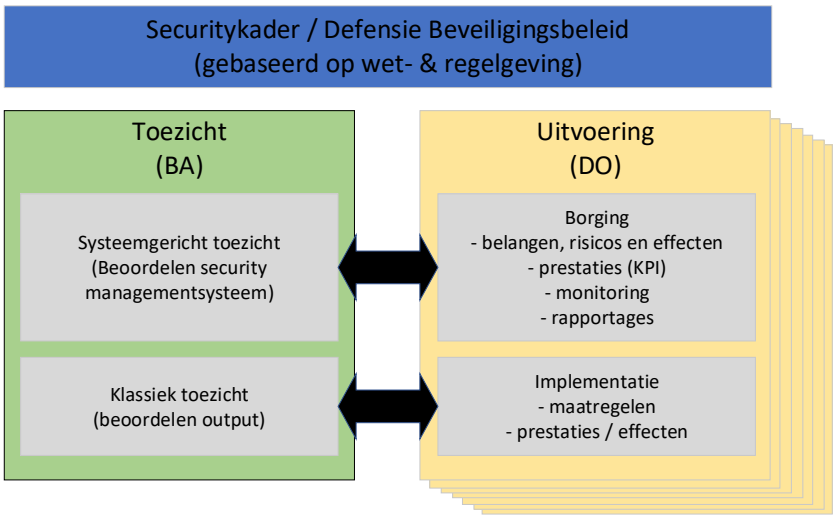
Het Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando (JISTARC) zal een securitykennisforum inrichten, genaamd Defensie Security Overleg (DSO), om toekomstgericht te gaan werken en aan te sluiten bij de modernisering van de krijgsmacht conform de Defensievisie 2035. De BA ondersteunt deze ontwikkeling.

2 Gehanteerde toezichtmethodiek

2.1 Positionering en taak van de BA

De SG heeft de Directeur Bedrijfsvoering & Evaluatie aangewezen als de departementale beveiligingsambtenaar (Beveiligingsautoriteit - BA). De DBE is daarmee verantwoordelijk voor de ontwikkeling van beveiligingsrichtlijnen (normenkaders) en het toezicht op de naleving daarvan.

De uitvoering van het toezicht op integrale beveiliging is door gemandateerd naar het afdelingshoofd Beveiliging, Gegevensbescherming en Documentaire Informatievoorziening. De BA is belast met het uitvoeren van toezicht en geeft daarmee invulling aan tweedelijns toezicht. Eerstelijns toezicht voeren de defensieonderdelen zelf uit. Zie ook onderstaand figuur.



De BA voert twee soorten toezicht uit:
Klassiek toezicht is outputgericht: bij klassiek toezicht beoordeelt de BA in hoeverre met de getroffen beveiligingsmaatregelen wordt voldaan aan de DBB-normeringen. Deze vorm van toezicht wordt veelal op locatie uitgevoerd en/of in samenwerking met ter zake deskundigen.
Systeemgericht toezicht is procesgericht: bij systeemgericht toezicht kijkt de BA met name naar de inrichting van processen 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 werking van een securitymanagementsysteem, en de mate waarin de PDCA-cyclus is gewaarborgd.

2.2 Meer nadruk op systeemgericht toezicht

Alle toezichtactiviteiten die in 2020 zijn uitgevoerd, waren aangekondigd. Daarbij is rekening gehouden met overige toezichtactiviteiten van de defensieonderdelen om dubbel werk te voorkomen. Het toezicht dient om vast te stellen of de commandanten en lijnmanagers het DBB juist naleven en om beveiligingsfunctionarissen te assisteren met kennis en advies.

Het klassieke toezicht richt zich op de feitelijke naleving van het DBB. De BA heeft onvoldoende capaciteit om bij alle defensieonderdelen volledig klassiek toezicht (toezicht op de output) uit te voeren. Door meer gebruik te maken van systeemgericht toezicht kan het klassieke toezicht worden beperkt tot steekproeven op basis van een risicoanalyse. Hierdoor komt meer nadruk te liggen op het eerstelijnstoezicht door de defensieonderdelen en de mate waarin zij de PDCA-cyclus borgen.

De BA registreert aanbevelingen / verbeterpunten naar aanleiding van uitgevoerd toezicht in een verbetertool. Deze tool is nog in ontwikkeling maar vormt een belangrijke basis voor het sluiten van de PDCA-cyclus.

2.3 Eventuele bijstelling van de norm

Als uit bevindingen van toezichtbezoeken blijkt dat een norm uit het DBB niet uitvoerbaar is, informeert de BA de procesmodeleigenaar (PME) beveiliging hierover. Indien nodig wordt de norm dan aangepast.

3 Toezicht 2020

Het toezicht van de BA was tot en met 2018 gebaseerd op klassiek toezicht (toezicht op de output). In 2019 is bij alle defensieonderdelen een koerswijziging ingezet richting systeemgericht toezicht. Bij deze vorm van toezicht beoordeelt de BA de aanwezigheid, de opzet en de werking van een securitymanagementsysteem bij de defensieonderdelen. Daarbij kijkt de BA naar de aanwezigheid van benodigde capaciteiten, lopende processen, documentatie, houdt zij interviews en voert ze steekproeven uit om vast te stellen of het securitymanagementsysteem voldoet en de PDCA-cyclus is gewaarborgd.

3.1 Systeemgericht toezicht met heldere normen

De afgelopen jaren hebben de defensieonderdelen het nodige voorwerk gedaan zoals het intensiveren van toezicht door de defensieonderdelen zelf (eerstelijns toezicht) en heeft de BA meer systeemvragen 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 elementen van het benodigde securitymanagementsysteem en naar de beheersingsmaatregelen die een defensieonderdeel heeft geïmplementeerd om aan het DBB te voldoen.

Door de uitbraak van Covid-19 en de diverse maatregelen met als doel het aantal contactmomenten te minimaliseren, heeft de BA in 2020 besloten om systeemgericht toezicht vooral digitaal uit te voeren. Hiertoe heeft zij een vragenlijst ontwikkeld die per defensieonderdeel inzicht geeft in de aanwezigheid, opzet en werking van een securitymanagementsysteem, of en hoe beveiligingsrisico's inzichtelijk zijn, hoe deze worden beheerst, et cetera.

Het DBB bevat beveiligingsnormen en kaders waaraan moet worden voldaan terwijl het defensieonderdeel verantwoordelijk is voor het inrichten van het beveiligingsmanagementsysteem. Er is dus een duidelijke scheiding tussen het 'wat' en het 'hoe'. Het DBB bevat echter geen normen en kaders waar een securitymanagementsysteem minimaal aan moet voldoen. Dat levert defensiebreed verschillen op. Dit is ook gebleken na het analyseren van de antwoorden op de vragenlijst en maakt het lastig om een securitymanagementsysteem te beoordelen.

De BA gaat daarom in 2021 - met behoud van inrichtingsvrijheid - een DBB-toezichtinstructie voor de Defensieonderdelen ontwikkelen.

De belangrijkste geconstateerde verschillen zijn:

- wel en geen eigen beveiligingsbeleid, regelgeving, visies en interpretaties;
- centraal en decentraal inzicht en beheersing van beveiligingsrisico's;
- beveiliging wel en niet geïntegreerd / geborgd in de interne rapportagestructuur;
- verschil in opzet, borging en uitvoering van een security-awarenessprogramma's en
- centraal en decentraal beheer van beveiliging voor de deelgebieden: Fysieke & Personele beveiliging, Informatiebeveiliging en Industrieveiligheid.

Naast de geconstateerde verschillen zijn er ook overeenkomsten die vooral zijn gerelateerd aan gestandaardiseerde beveiligingsprocessen, generieke informatievoorziening en/of de afhankelijkheid van interne en/of externe dienstverleners.

Het inzicht dat de vragenlijst opleverde, wordt gebruikt voor volgende toezichtbezoeken waarbij verder en dieper zal worden ingegaan op de securitymanagementsystemen bij de defensieonderdelen.

3.2 Deelgebied Fysiek & Personeel

Investeren in kennis Bouwmatrix noodzakelijk

De bouwmatrix is een op beveiligingsnormen gebaseerde set met bouwtechnische beveiligingsmaatregelen. Het beheer van de bouwmatrix is sinds enkele jaren belegd bij het Rijksvastgoedbedrijf (RVB). Voorheen was dit bij Defensie Ondersteuningscommando / Divisie Vastgoed Defensie (DOSCO/DVD). Doordat de DVD enkele jaren geleden is overgegaan naar het RVB is de kennis over de bouwmatrix bij Defensie weggevloeid. RVB probeert de matrix bij te houden met ondersteuning vanuit Defensie. Echter, de kennis die hiervoor benodigd is, staat door reorganisaties bij Defensie onder grote druk. Als de kennis in het geheel verdwijnt is er een substantieel risico dat het RVB de matrix niet meer kan beheren. Investeringen in het behoud van gekwalificeerd personeel zijn daarom noodzakelijk.

Verwerking van Defensie vastgoedinformatie door het RVB

De BA heeft in 2020 samen met het RVB op de negen locaties van het RVB een schouw uitgevoerd om vast te stellen welke maatregelen nodig zijn om Defensie vastgoedinformatie (analoog en digitaal) veilig te kunnen verwerken. Van de schouw is een verslag opgesteld met aandachts- en verbeterpunten. Het RVB implementeert, in samenwerking met Defensie, momenteel de verbetermaatregelen.

Defensie Bewakings- en Beveiligingssysteem (DBBS) is vertraagd
Het project DBBS heeft te kampen met vertragingen. Daardoor moeten bestaande en verouderde toegangs- en/of beveiligingssystemen in stand worden gehouden. Het is van groot belang dat er geen verdere vertraging in de ontwikkeling en implementatie van DBBS ontstaat. De BA monitort de verdere voortgang.

Capaciteit DBBO ontoereikend / onder spanning
De Defensie Bewakings- en Beveiligingsorganisatie (DBBO) is structureel onderbezet en daarom is er steeds spanning op de formatie en de taken. Om het personeelsbestand uit te breiden heeft DBBO in 2016 de Commandant der Strijdkrachten verzocht om extra financiële middelen voor personele capaciteit. Daarnaast is het voor DBBO ook van belang dat bij de start van projecten wordt nagedacht over eventuele consequenties voor de dienstverlening van DBBO, en dat de benodigde financiële middelen tevoren zijn gereserveerd.

Versterking samenhang en kwaliteit beveiligingsketen is noodzakelijk
Binnen de gehele beveiligingsketen wordt onderkend dat de kennis en capaciteit in de loop der jaren achter is gebleven bij de ontwikkelingen. Dit komt door de diverse reorganisaties, waardoor capaciteit en kwalitatief goed personeel wegstroomden. Binnen het Inlichtingen & Veiligheid (I&V) functiegebied binnen Defensie is er het Defensie Inlichtingen en Veiligheidsoverleg (DIVO). De nadruk binnen dit overleg ligt op het deel Inlichtingen. Binnen het DIVO en de gehele I&V keten, krijgt veiligheid (lees beveiliging/security) onvoldoende aandacht en de noodzakelijke samenhang binnen I&V is onvoldoende. Daarom zal er een nieuw functioneel overleg worden ingericht onder het DIVO: het DSO (Defensie Security Overleg). Het Kenniscentrum I&V JISTARC zal de voorzitter van dit DSO ondersteunen en de vulling verder realiseren vanuit de defensieonderdelen. Het doel is innovatiever en toekomstgerichter te gaan werken om aan te sluiten bij de modernisering van de krijgsmacht conform de Defensievisie 2035. De BA heeft dit punt in de appreciatie van de managementrapportage opgenomen.

Elektronische Veiligheidsonderzoeken onvoldoende
Elektronische Veiligheidsonderzoeken worden ingezet om uit te sluiten dat er ongeautoriseerd kan worden meegeluisterd met hoog gerubriceerde gesprekken in gerubriceerde ruimtes. De onderzoekscapaciteit is op dit moment onvoldoende om aan de vraag te kunnen voldoen.

3.3 Toezicht F-35 programma: voldoende

In 2020 heeft de Nederlandse Program Security Officer (PSO) vanuit de BA alle Special Access Program Facilities 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 informatie binnen het F-35 programma de merking Special Access Required. Deze informatie wordt op te beschermen belang -categorie 1- beveiligd en mag uitsluitend verwerkt worden in de hierboven genoemde Special Access Program Facilities. Op grond van de toezichtbezoeken heeft de BA alle Special Access Program Facilities op gebied van integrale beveiliging als voldoende beoordeeld.

3.4 Informatiebeveiliging

Accreditatie kritieke systemen grotendeels op orde

De accreditatiestatus van de kritieke informatiesystemen is sinds 2017 gelijk gebleven. Voor elf kritieke systemen is een tijdelijke goedkeuring gegeven met de aanvullende voorwaarden dat de nog te implementeren beveiligingsmaatregelen worden verwerkt in een verbeterplan en dat vóór het verstrijken van de tijdelijke goedkeuring een her-accreditatieaanvraag moet zijn ingediend. Deze aanvragen zijn beoordeeld en voor de meeste systemen geldt dat er voortgang is maar nog niet voldoende voor een accreditatie. Voor de overige drie kritieke systemen is een accreditatie verleend.

Beoordeling Algemene Rekenkamer (AR) over informatiebeveiliging

De AR en Audit Dienst Rijk (ADR) voeren elk jaar een audit uit op de status van de informatiebeveiliging binnen het Rijk. De Chief Information Officer (CIO), JIVC en BA hebben wederom intensief samengewerkt om de vragen van de AR te beantwoorden en de vereiste onderbouwing aan te leveren. De ADR en AR hebben dit beoordeeld en een aantal aanbevelingen gedaan.

Centrale sturing op informatiebeveiliging

In november heeft de ADR de centrale sturing op de informatiebeveiliging getoetst op basis van een rijksbreed afgesproken maturity-model. Voor dit jaar is het aantal onderwerpen teruggebracht tot risicomanagement. Voor dit onderwerp had Defensie eerder de ambitie uitgesproken om hiervoor op niveau 3 (van vijf niveaus) uit te willen komen - in analogie met de andere onderwerpen die in voorgaande jaren zijn beoordeeld: governance, organisatie en incidentmanagement.

CIO, JIVC en BA hebben hierbij samengewerkt om dit maturity-model in te vullen en de benodigde onderbouwing aan te leveren. Daaruit zijn geen urgente aandachtspunten naar voren gekomen. Defensie pakt de aanbevelingen uit het rapport in 2021 verder op; deze worden opgenomen in het verbetermanagementsysteem van JIVC zodat de voortgang kan worden gemonitord. Daarmee wordt de in het kwaliteitssysteem IT beschreven verbetercyclus versterkt.

Nieuwe impuls programma Grensverleggende IT

In 2014 is geconstateerd dat de staat van de IT bij Defensie een risico vormt voor de continuïteit van de dienstverlening en bedrijfsvoering. Om de continuïteit op de lange termijn te garanderen is besloten de IT-infrastructuur de komende jaren volledig te vernieuwen met het programma Grensverleggende IT (GrIT). Deze vervanging laat echter langer op zich wachten dan aanvankelijk voorzien. Het is van belang dat binnen het project, beveiliging vanaf de start integraal wordt gewaarborgd in de op te leveren IT-diensten en dat wordt nagedacht over eventuele consequenties voor kwaliteit en kennis van de beveiligingsketen. De aanbesteding is eind 2020 afgerond, waardoor Defensie kan gaan bouwen aan een nieuwe goed beveiligde en toekomstbestendige infrastructuur.

Beschikbaarheid tempestproducten

Verworven producten waar tempesteisen (eisen om te voorkomen dat informatie via straling lekt) op van toepassing zijn, blijken kwalitatief onvoldoende. Hierdoor is spanning ontstaan op de beschikbaarheid van deze producten. Dit probleem is onderkend en heeft de aandacht van de BA. Er wordt gewerkt aan een toekomstbestendige oplossing.

3.5 NAVO-Inspectie voornamelijk positief

In 2019 heeft NAVO een inspectie uitgevoerd met als doel de beveiliging van (gerubriceerde) NAVO-informatie te inspecteren op de eisen die NAVO hieraan stelt. De betrokken Defensielocaties waren het Plein-Kalvermarkt Complex in Den Haag en de gemeenschappelijke Permanente Vertegenwoordiging in Brussel. Ook werd een Defensiepartner geïnspecteerd, TNO in Den Haag. Naast Defensie zijn ook de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, van Buitenlandse Zaken, en van Infrastructuur en Waterstaat geïnspecteerd. Het NAVO-inspectieteam rapporteerde grotendeels positief, er waren enkele aanbevelingen. Deze aanbevelingen zijn door de BA omgezet naar acties ter verbetering. Deze acties ter verbetering zijn door de BA opgenomen in de verbetertool en worden door de BA gemonitord.

3.6 EU-Inspectie

Van 10 tot en met 15 oktober 2019 heeft een team van EU-inspecteurs onderzocht of (gerubriceerde) EU-informatie adequaat behandeld en beveiligd wordt. Evenals bij de NATO-inspectie bezocht het EU-inspectieteam meerdere departementen. Betrokken defensielocaties waren het Plein-Kalvermarkt Complex en de Koningin Máximakazerne op Schiphol. De bevindingen van de EU-inspectie komen grotendeels overeen met de bevindingen van de NAVO-inspectie. Het EU-inspectieteam heeft een positief verslag opgesteld met aanvullend enkele aanbevelingen. Deze aanbevelingen zijn door de BA omgezet naar acties ter verbetering. Deze acties ter verbetering zijn door de BA opgenomen in de verbetertool en worden door de BA gemonitord.

4 Samenwerking

4.1 Samenwerking met de Functionaris Gegevensbescherming (FG)

In 2020 zijn vanwege de Covid-19 situatie geen fysieke toezichtbezoeken uitgevoerd in samenwerking met de Functionaris Gegevensbescherming (FG). De BA is in 2020 wel betrokken bij een aantal door de FG geïnitieerde onderzoeken.

Centrum voor Arbeidsverhoudingen Overheidspersoneel (CAOP): minder intensief toezicht nodig

De BA voert gezamenlijk toezicht met de FG uit bij het Centrum voor Arbeidsverhoudingen Overheidspersoneel (CAOP), in het kader van opslag persoonsgegevens voor het onderzoek naar gezondheidsklachten van (oud-) medewerkers van Defensie. Eerder heeft de BA vastgesteld dat het CAOP grotendeels voldoet aan de vastgestelde beveiligingsnormen zoals beschreven in de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Rijksdienst (BIR). Ook heeft de FG in 2020 geconstateerd dat de verbetermaatregel om te komen tot een Data Protection Impact Assessment (DPIA), bijna afgerond is. Daarom, en vanwege de aangescherpte COVID-19-maatregelen, hebben de BA en de FG gezamenlijk besloten het (intensieve) toezichttraject af te sluiten en over te gaan naar reguliere invulling van de toezichtrol.

Land Information Manouvre Center (LIMC): BA ondersteunt FG

Naar aanleiding van de berichtgeving over de activiteiten van het LIMC in NRC Handelsblad op 16 november 2020, voert de FG een onderzoek uit naar de naleving van de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG bij het LIMC. De BA is bij dit onderzoek betrokken en ondersteunt de FG bij het beoordelen van de technische en organisatorische beveiligingsmaatregelen die het LIMC neemt om persoonsgegevens op een veilige manier te verwerken, zoals bedoeld in artikel 32 van de AVG. Dit onderzoek loopt vanwege de omvang door in 2021. De BA brengt over de voortgang en inhoud van het onderzoek geen afzonderlijk verslag uit omdat haar bijdrage het onderzoek van de FG betreft die hierover zal rapporteren. Deze samenwerking verloopt vanaf de start van het onderzoek professioneel en constructief.

4.2 Samenwerking met Bureau Industrieveiligheid is effectief

Bedrijven die zijn belast met de uitvoering van gerubriceerde en/of vitale defensieopdrachten, dienen te voldoen aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). BIV (Bureau Industrieveiligheid) van de MIVD houdt hier toezicht op in de rol van Designated Security Authority (DSA).

Door diverse Covid-19 maatregelen die als doel hebben het aantal contactmomenten te minimaliseren, heeft BIV in samenspraak met de BA besloten de uitvoering van toezicht bij de bedrijven tot het strikt noodzakelijke te beperken. De daadwerkelijk uitgevoerde audits waren gerelateerd aan accreditaties en her-audits in opdracht van de BA. De resultaten van de audits waren overwegend positief en er kan worden geconcludeerd dat de audits van de afgelopen jaren een belangrijke bijdrage hebben geleverd aan de noodzakelijke verhoging van het integrale beveiligingsniveau bij de bedrijven die belast zijn met de uitvoering van gerubriceerde en/of vitale defensieopdrachten. De samenwerking tussen het BIV en de BA in 2020 was goed en intensief, met name tijdens de uitvoering van de her-audits.

4.3 Samenwerking met DBBO verloopt goed

In het kader van samenwerking en afstemming toezichtprocedures, zal de BA in de toekomst betrokken worden bij de Red Teaming activiteit, genaamd “Operatie Waakhond”, die DBBO (Defensie Bewakings- en Beveiligingsorganisatie) binnen de eigen organisatie uitvoert. In 2020 heeft de oefening wel plaatsgevonden maar is de BA vanwege de Covid-19-situatie niet fysiek bij de oefening aanwezig geweest. De Red Teaming activiteit in 2020 is uitgevoerd op achttien locaties waarbij de interventietijden en de controle van de Lokale Beveiligingsinstructie (LBI) centraal stonden. Ook is communicatie en de onderlinge samenwerking beoordeeld. Van de test heeft DBBO een verslag gemaakt met bevindingen. DBBO heeft reeds verbeteracties geïnitieerd en monitort ze ook zelf. Daar waar de bedrijfsvoering van een defensieonderdeel verbeterd zou kunnen worden, neemt DBBO contact op met de desbetreffende beveiligingscoördinator.

4.4 Samenwerking met AIVD intensiever en beter

De BA voert samen met de AIVD toezicht uit bij de beide diensten (MIVD en AIVD); ook worden gezamenlijk informatiesystemen geaccrediteerd. Dit verbetert de samenwerking en het vertrouwen. De beoordeling van locaties in 2020 stond in het teken van controles van een aantal locaties in Nederland maar ook daarbuiten. Deze locaties zijn van een accreditatie voorzien. Daarnaast is op frequente basis overleggen geregeld om de status van de informatiesystemen te bespreken en te beoordelen met als doel te komen tot wederzijds geaccrediteerde informatiesystemen.

4.5 Samenwerking met RijksBVA verloopt naar verwachting

Het BVA-beraad, een samenwerkingsverband tussen beveiligingsautoriteiten van de verschillende departementen, heeft als doel verschillende beveiligingsonderwerpen te bevorderen, zoals toezicht, security-awareness, risicomanagement, proactieve beveiliging etc. In relatie tot toezicht werken de BVA's daartoe samen met andere toezichthoudende functies en laten ze fysieke beveiligingstesten binnen hun departementen uitvoeren.

Fysieke beveiligingstesten

De RijksBVA heeft een contract afgesloten met een externe partij die de BVA's ondersteunt. Dit meerjarig contract biedt rijksbreed de mogelijkheid drie tot zes beveiligingstesten per jaar te laten uitvoeren. De BA heeft in samenwerking met het Commando Landstrijdkrachten (CLAS) een fysieke beveiligingstest georganiseerd en uitgevoerd waarbij gebruik is gemaakt van het door de RijksBVA aangeboden contract. Deze vorm van samenwerken met de RijksBVA en het positieve resultaat van de test hebben geresulteerd in een meerbehoefte voor de komende jaren.

Security Awareness

Onder de vlag van het BVA-beraad werken verschillende Interdepartementale werkgroepen binnen de beveiligingsketen specifieke onderwerpen uit. Deze werkgroepen zijn verdeeld in zogenaamde *fiches*. Fiche 3 gaat over het rijksbrede programma security-awareness onder leiding van het Ministerie van Buitenlandse Zaken en het Ministerie van Defensie. Dit fiche ontplooit diverse initiatieven om de beveiligingsbewustwording rijksbreed te vergroten; voor deze activiteiten is goedkeuring van de Interdepartementale Beveiligingsraad (IBR) nodig. Er is eerder onderzoek verricht naar gedragsverandering en er zijn binnen de verschillende ministeries diverse thema-artikelen in relatie tot beveiliging rijksbreed gepubliceerd. Fiche 3 werkt conform een door het BVA-beraad goedgekeurd jaarplan.

Nationale Crypto Strategie

Defensie werkt in interdepartementaal verband samen aan een Nationale Crypto Strategie (NCS). Deze strategie beschrijft hoe ook in de toekomst cryptografische beveiligingsmaatregelen, om gevoelige informatie te beschermen, voor de gehele rijksoverheid beschikbaar blijven.