BS/2011005174 / 16-2-2011

Ministerie van Defensie

D-DMO
MPC 58 A
Postbus 90826
2509 LV Den Haag

Supervisor SPEER
VADM J.G. van der Burg
MPC 58 A
Postbus 90822
2509 LV Den Haag

Audit Dienst Defensie
ERP/M&F

Spui 32
MPC 58 B
Postbus 20701
2500 ES Den Haag
Nederland
www.defensie.nl

nota

Onderzoek autorisaties MATLOG

Datum
28 februari 2011

Onze referentie
BS/2011005174

Afschrift aan
Zie verzendlijst

Bij beantwoording datum, onze referentie en betreft vermelden.

Bijlage
1

Een belangrijk onderdeel van de inrichting van SAP is de toekenning van autorisaties. Om ongewenste functievermenging en ongeautoriseerde toegang tot gevoelige informatie te voorkomen is de toekenning van rechten in SAP (autorisaties) essentieel. Uitgangspunt is dat dit zoveel mogelijk uniform gebeurt om de geïntegreerde bedrijfsvoering te ondersteunen.

De huidige inrichting dreigt echter het paars werken c.q. geïntegreerde bedrijfsvoering onvoldoende te ondersteunen. In de praktijk treffen we een "explosie" van rollen aan wat bovendien een verzwaring betekent voor het (toekomstig) beheer en onderhoud. Tot nu toe is door de DMO nog niet voldoende invulling gegeven aan haar richtende en inrichtende rol voor autorisaties MATLOG. Uitvoeringsbepalingen, zoals de HDFC heeft opgesteld voor inrichten en beheer van F autorisaties, ontbreken nog.

Daar functiescheiding en daaraan gerelateerde autorisaties prominente beheersmaatregelen zijn, vragen wij dan ook aandacht voor de in het bijgevoegde rapport van bevindingen opgenomen bevindingen en adviezen.

DE PLV. DIRECTEUR AUDITDIENST DEFENSIE

E. van Vught RA
Brigade-generaal

Ministerie van Defensie

Audit Dienst Defensie
ERP / M&F

Datum
28 februari 2011

Onze referentie
BS/2011005174

Contactpersoon
Drs. J.Schoonen RA RE MGA
V.E. Toms RE

verzendlijst

In afschrift aan

SG
MPC 58 B
Postbus 20701
2500 ES Den Haag

HDFC
MPC 58 B
Postbus 20701
2500 ES Den Haag

DMO/ST/TM

MPC 58 A
Postbus 90826
2509 LV Den Haag

MPC 58 A
Postbus 90826
2509 LV Den Haag

CDC/IVENT

MPC 55 A
Postbus 90004
3509AA Utrecht

Transitiemanager/Hoofdproject Data

MPC 58 A
Postbus 90822
2509 LV Den Haag

Ministerie van Defensie

Audit Dienst Defensie

Datum
28 februari 2011

Onze referentie
BS/2011005174

bijlage

RAPPORT VAN BEVINDINGEN AUTORISATIEBEHEER MATLOG

1. Inleiding/achtergrond

De huidige taakstelling van Defensie is primair gericht op operationeel joint optreden ten behoeve van vrede en veiligheid wereldwijd. Joint optreden vereist ook joint ondersteuning.
Defensie heeft voor ondersteuning op het logistieke en financiële vlak gekozen voor het ERP-systeem SAP. Wil SAP het joint optreden van Defensie kunnen ondersteunen, dan is het noodzakelijk dat SAP defensiebreed uniform wordt ingericht en dat de ingerichte functionaliteiten van SAP aansluiten bij de bestaande visie op joint optreden alsmede de richtlijnen omtrent het beheer van materieel.

Een belangrijk onderdeel van de inrichting van SAP is de toekenning van de autorisaties. Enerzijds wordt middels het uniform toekennen van autorisaties het paars werken ondersteund, en daarmee de geïntegreerde bedrijfsvoering. Anderzijds dient een adequate inrichting van de autorisaties te voorkomen dat ongeautoriseerden toegang verkrijgen tot "gevoelige" informatie over materieel.

In dit licht is door de ADD eind 2010 een onderzoek uitgevoerd naar de opzet van het autorisatiebeheer SAP MATLOG. Het doel van het onderzoek was het maken van een inventarisatie van de in opzet aanwezige beheersmaatregelen betreffende het richten en inrichten van autorisaties SAP MATLOG.

Er is geen onderzoek uitgevoerd naar de daadwerkelijke inrichting (bestaan) van autorisaties MATLOG in SAP.
Gezien de beperkt beschikbare tijd heeft dit onderzoek een beperkte diepgang. Het onderzoek resulteert dan ook in bevindingen en niet tot een totaal oordeel. Er is geen sprake van een assurance opdracht.

In dit rapport gaan wij in op de belangrijkste bevindingen uit ons onderzoek welke met uw contactpersoon Dhr. B. Sax van der Weijden zijn doorgesproken.

2. Belangrijkste bevindingen

Onderstaand wordt ingegaan op de belangrijkste bevindingen voortvloeiend uit het onderzoek.

De belangrijkste bevindingen zijn:

- Tot op heden is door DMO nog onvoldoende structureel invulling gegeven aan haar richtende en inrichtende rol t.a.v. autorisatiebeheer MATLOG. In dit licht is het van belang dat er een aangewezen functionaris voor het autorisatiebeheer MATLOG wordt aangesteld die integraal verantwoordelijk is voor richten en inrichten van MATLOG autorisaties. Gemist wordt een vanuit de beleidsverantwoordelijke centrale overkoepelende aansturing van het richten en inrichten van autorisaties MATLOG. Deze centrale aansturing vanuit de beleidsverantwoordelijke is van essentieel belang voor het borgen van de aansluiting met de gedachtegang van de beleidsverantwoordelijke omtrent het paars werken c.q. geïntegreerde bedrijfsvoering . Er is behoefte aan een vertaalslag van visie en richtlijnen naar een concreet normenkader voor de inrichting van autorisaties.
  Naast het aanwijzen van voornoemde functionaris is het wenselijk dat eenduidig is vastgelegd welke partijen zijn betrokken bij het beheer van autorisaties (DMO, CDS, HDFC, BF-IVENT, SPEER etc.) alsmede wie welke taak, verantwoordelijkheid en bevoegdheid heeft. Tevens is het wenselijk dat er concrete (contact)personen worden aangewezen.

- Momenteel is er slechts een beperkt aantal partijen (actief) betrokken bij de invulling van autorisatiebeheer MATLOG. Vanuit de beleidsverantwoordelijken DMO en CDC is er momenteel weinig inbreng. Er is geen formeel structureel overleg autorisaties MATLOG waarbij de richtende en inrichtende partijen alsmede de beheerders aanzitten. Een dergelijk overleg is van belang voor het Defensiebreed neerzetten van autorisaties MATLOG en om te komen tot Defensiebrede keuzes/oplossingen. Tevens kan een dergelijk forum dienen als platform voor het oplossen van issues ter voorkoming van procesverstoring c.q. procesfrustratie, alsmede voor het borgen van het op elkaar aansluiten van autorisaties MATLOG en FINAD.

- Er ontbreekt momenteel een "overkoepelende" norm (autorisatiematrix) die als basis dient voor de inrichting en toekenning van autorisaties MATLOG. Zie in dit licht als bijvoorbeeld het door HDFC uitgegeven normenkader. Een dergelijke norm is ook van belang als basis voor het gestructureerd testen van gewijzigde/ nieuwe rollen en voor het structureel monitoren van de toegekende autorisaties (zowel vooraf bij toekenning als achteraf als toetsing van de functiescheiding binnen de productieomgeving). Op dit moment is vanuit de beleidsverantwoordelijke niet voorzien in een gestructureerde monitoring van c.q. toezicht op autorisaties MATLOG.

- Vanuit het programma SPEER probeert het project AO/IC in samenwerking met BG-Ivent de leemtes zo goed mogelijk op te vangen. De opgeleverde procesbeschrijving (ARIS) door SPEER/OBBS is gebruikt als basis voor het inrichten van de MATLOG autorisaties.

- Momenteel bestaan er verschillen tussen de wijze van inrichten van autorisaties voor de functionele gebieden FINAD en MATLOG. Waar bij FINAD voor de inrichting van composite rollen is gekozen voor het niveau van een functie (waarbij taken zijn samengevoegd tot een functie), wordt bij MATLOG ook composite rollen op het niveau van taken ingevuld. Daarnaast vindt binnen autorisaties MATLOG afscherming van wapensystemen niet plaats op basis van het principe afgeleide rollen maar op basis van zogenaamde "verdiepte kernelrollen" (specifiek per wapensysteem). Deze kernelrollen (alsmede wijzigingen hierop) kunnen niet van een template worden afgeleid.
  Beide punten hebben geleid tot een explosie van rollen voor het MATLOG-gebied. Dit betekent een verzwaring van het (toekomstig) beheer & onderhoud en potentieel risico voor het overschrijden van het maximaal toe te kennen rollen aan één gebruiker.

- Door het bottom up ontwikkelen van MATLOG-rollen (voor de defensie-onderdelen Zee, Lucht en Land) dreigen er verschillende rolconcepten te ontstaan. Naast een toename van rollen (en daarmee een toename van de beheerlast) kan dit het paars werken bemoeilijken.

3. Adviezen

Op grond van de hiervoor vermelde observaties hebben wij de volgende adviezen:

- Het binnen DMO aanwijzen van een functionaris die integraal verantwoordelijk is voor het richten en inrichten van MATLOG autorisaties
- Het in kaart brengen van de partijen betrokken bij autorisatiebeheer MATLOG en eenduidig vastleggen wie welke taak, verantwoordelijkheid en bevoegdheid heef t.a.v. autorisaties SAP MATLOG. In dit licht tevens aanwijzen van functionarissen.
- Het invoeren van een structureel overleg waarbij voornoemde functionarissen (met mandaat) zitting hebben.
- Het met voorrang ontwikkelen van een defensiebreed normenkader autorisaties MATLOG, dat aansluit bij visie en richtlijnen en geaccordeerd is door de beleidsverantwoordelijke DMO.
- Het op basis van het overeengekomen normenkader inrichten van tools ten behoeve van testen en monitoring. Het vervolgens structureel inbedden van toezicht / monitoring binnen de organisatie. Als voorbeeld wordt verwezen naar het door HDFC uitgegeven normenkader voor de financiële processen
- Het uitvoeren van een fit-gap analyse (feitelijke en wenselijk geachte autorisaties MATLOG) en het met voorrang op één lijn brengen van de inrichting van de autorisaties
- Het onderzoeken van de mogelijkheid om de autorisaties wapensysteem op te zetten volgens het principe van afgeleide rollen, danwel het zoeken naar andere (beheersbare) alternatieven
- Het omarmen van het principe van definiëren van composite roles op het niveau van een functie en het uitvoeren van een opschoningslag in deze.