AUDIT MAGAZINE

ARTIKELEN | 3 JULI 2023

DE AUDITOR ALS INBREKER

Auteur: Dr. Sjoerd Keulen – Tom van der Meijden MSc
Beeld: Ministerie van Defensie - Algemene Rekenkamer
Leestijd: 8 min

Defensie beschikt over grote voorraden wapens, munitie en geheime informatie. Die mogen niet in verkeerde handen vallen. Een aanslag op straaljagers, marineschepen of commandocentra kan de krijgsmacht verlammen. Beveiliging is daarom van belang. Door de oorlog in Oekraïne is de staat van waakzaamheid bovendien verhoogd en de beveiliging aangescherpt.

De Algemene Rekenkamer heeft de beveiliging van een aantal militaire objecten daarom getest als onderdeel van het jaarlijkse verantwoordingsonderzoek dat op 17 mei 2023 is gepresenteerd aan de Tweede Kamer. De audit bij Defensie kreeg veel aandacht van Kamerleden en pers: 'De nerds van de rekenkamer blijken over hekken te klimmen', aldus verbaasde *EenVandaag*-presentatoren van deze actualiteitenrubriek. 'Niks geen saaie accountants', aldus het ludieke tv-programma *Even tot Hier*, maar 'The A-Team', 'nooit geweten dat die boekhouders dat zelf testen'.

Derde woensdag in mei

De Algemene Rekenkamer presenteert ieder jaar op de derde woensdag in mei haar bevindingen over de rechtmatigheid van de uitgaven van het rijk en over de stand van de bedrijfsvoering op de departementen. Zaken in de bedrijfsvoering die niet voldoen worden als 'onvolkomenheden' aangemerkt. Het parlement kan dit verantwoordingsonderzoek gebruiken voor de dechargeverlening aan de minister.

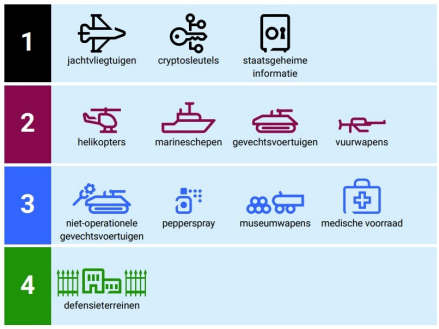
'Niks geen saaie accountants', aldus het ludieke tv-programma *Even tot Hier*,

maar ‘The A-Team’

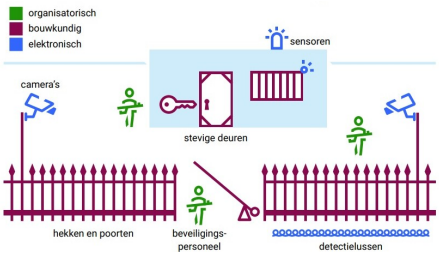
Vanwege de verbazing van de buitenwacht en omdat deze auditmethode een interessante toevoeging kan zijn voor de gereedschapskist van de internal auditor, lichten wij in dit artikel graag toe wat de aanleiding was voor dit onderzoek en hoe we opzet, bestaan en werking van objectbeveiliging hebben onderzocht. Vervolgens gaan we in op de onderzoeksmethode en de belangrijkste uitkomsten van onze audit.

Van risico naar test

Door de oorlog in Oekraïne is de dreiging in West-Europa groter geworden. Niet voor niets is na de Russische inval de waakzaamheid op defensieterreinen verhoogd tot Alert State Alpha. Vorig jaar bleek uit ons onderzoek al dat het relatief makkelijk was om munitie te ontvreemden bij Defensie. Tegen die achtergrond en omdat de goede zorg voor materieel een van de vaste onderwerpen van het verantwoordingsonderzoek van de Algemene Rekenkamer is, hebben we er ditmaal voor gekozen om te onderzoeken hoe het staat met de beveiliging van de belangrijkste defensieobjecten.



Bij Defensie zijn vier niveaus van te beschermen belangen



De beveiliging van Defensie bestaat uit drie soorten maatregelen

We hebben specifiek onderzoek gedaan naar de beveiliging van de twee zwaarste categorieën van te beveiligen objecten. Deze objecten zijn (vrijwel) onmisbaar voor de krijgsmacht, bijvoorbeeld omdat er geen alternatieven zijn. Of het betreft staatsgeheimen waarvan de kennisname door niet-gerechtigden zeer ernstige gevolgen hebben voor de Nederlandse Staat en/of NAVO-bondgenoten. Het gaat bijvoorbeeld om operationele vliegtuigen, schepen en gevechtsvoertuigen, maar ook om datacentra, radarinstallaties of wapens.

In de wetenschap dat het verlies of beschadiging van deze militaire objecten een grote impact zou hebben op de krijgsmacht scoorde dit onderzoek hoog op onze risicoanalyse. Uit eerder onderzoek in 2003 en 2005 bleek ook al dat binnendringen bij Defensie mogelijk was. De Algemene Rekenkamer heeft al vaker gebruikgemaakt van dit type praktijkonderzoek om invulling te geven aan haar wettelijke taak en niet alleen bij Defensie.

Praktijktesten

Al in 1988 zette de Algemene Rekenkamer praktijktesten in. Het leidde tot een geruchtmakend rapport in aanloop naar de verzelfstandiging van rijksmusea. De Algemene Rekenkamer constateerde destijds dat kunst voor het grijpen lag doordat kluizen open stonden, depots niet altijd waren aangesloten op de beveiliging en insluipers via dienstingangen ongezien de panden kon betreden. Uit een ander onderzoek, in 2019, bleek dat insluipers bij controlekamers en servers van vitale waterwerken bij Rijkswaterstaat konden komen. En in 2020 bleek uit ons onderzoek naar de grensbewaking op Schiphol dat standaardwachtwoorden in gebruik waren en dat het mogelijk was om uit naam van defensiemedewerkers e-mails te versturen.

Standaardwachtwoorden

Standaardwachtwoorden zijn internationaal een probleem. Zo concludeerde de Amerikaanse Rekenkamer GAO op basis van pentesten bijvoorbeeld dat veel Amerikaanse wapensystemen nog steeds standaardwachtwoorden van de leveranciers gebruikten. Hackers konden zo binnen negen seconden het juiste wachtwoord raden. Praktijktesten van diezelfde GAO toonden in 2006 aan dat het gemakkelijk was om nucleair materiaal (bijvoorbeeld voor een vuile bom) de Verenigde Staten in te smokkelen.

Voor de Noorse Rekenkamer Riksrevisjonen behoren penetratietesten al acht jaar tot het standaardinstrumentarium en vielen zowel de Noorse politie als het Noorse olieagentschap na testen door de mand. Het onderzoek van de Algemene Rekenkamer naar de beveiliging van militaire objecten sluit in dat licht naadloos aan bij de trend in de internationale auditgemeenschap om overheidsprestaties in de praktijk te testen.

De kern van het beveiligingsbeleid van Defensie gaat uit van een combinatie van drie soorten beveiligingsmaatregelen: organisatorische, bouwkundige en elektronische

Opzet en bestaan. Werkt het ook?

De praktijktesten bij Defensie zagen we als het sluitstuk van ons onderzoek. Volgens de auditlogica van opzet, bestaan en werking zijn we eerst met de basis begonnen. De kern van het beveiligingsbeleid van Defensie gaat uit van een

combinatie van drie soorten beveiligingsmaatregelen: organisatorische, bouwkundige en elektronische. Samen moeten die een adequate beveiliging van de objecten vormen. De Algemene Rekenkamer oordeelde dat het beveiligingsbeleid goed is opgezet, systematisch is uitgedacht en actueel is. Daarmee voldoet de opzet.

Over het bestaan was de Rekenkamer minder enthousiast. Om het beleid uit te kunnen voeren, zijn voor de verschillende defensieonderdelen en locaties actuele beveiligingsplannen nodig. Door het gebruik van materieel in operaties, het verplaatsen en uitbreiden van wapensystemen en door verbouwingen is het belangrijk dat de plannen actueel zijn. Alleen wanneer beveiligingsrisico's bekend zijn kunnen er immers maatregelen genomen worden om deze op te lossen.

De beveiligingsfunctionarissen die deze plannen opstellen zijn echter schaars in de hele defensieorganisatie. Er zijn veel lege stoelen. Hierdoor zijn er achterstanden ontstaan in het actualiseren van de beveiligingsplannen. Defensie heeft daardoor geen actueel inzicht in de beveiligingsrisico's rondom de militaire objecten. Daarnaast controleert het ministerie niet of nauwelijks of de maatregelen uit de plannen daadwerkelijk leiden tot een adequate beveiliging, terwijl ze daar wel een goede systematiek voor hebben.

Operatie Waakhond

Voor de praktijktesten hebben we, samen met de Defensie Bewakings- en Beveiligingsorganisatie, gebruikgemaakt van de werkwijze van Operatie Waakhond, dat de Defensie Bewakings- en Beveiligingsorganisatie zelf heeft ontwikkeld en tot een paar jaar geleden ook gebruikte. Operatie Waakhond gaat uit van red teaming door middel van penetratietesten. Red teaming is ontstaan in de Koude Oorlog en bekend geworden door oorlogssimulaties van denktank RAND Corporation. Hier nam het blauwe team het op tegen de vijand, het rode team. Rode teams worden tegenwoordig ingezet als advocaat van de duivel die zich zoveel mogelijk inleven in de tegenstander en proberen in (oorlogs)simulaties tegenstand te bieden of bij beveiligingstesten binnen te dringen. Met het doel hiervan te leren en de organisatie te verbeteren.

Dreigingsrisico's

Voor onze testen werden bestaande dreigingsscenario's, waartegen de beveiligingsmaatregelen bestand moeten zijn, als uitgangspunt gebruikt. Deze vorm van testen heeft als voordeel dat het zowel de bouwkundige als de elektronische

beveiliging test, maar vooral ook de factor mens. Zo konden we vaststellen of en hoe waakzaam defensiemedewerkers zijn wat betreft ongenode gasten. Maar ook of bij detectie de bewaking binnen de voorgeschreven aanrijdtijden reageerde.

Auditors van de Rekenkamer konden in het observatieteam continu de inbraakpogingen nauwgezet volgen en ontvingen naderhand de ongefilterde rapportage

De testen werden, onder regie van de Algemene Rekenkamer, door vrijgestelde defensiemedewerkers voorbereid en verkend. Om veiligheidsrisico's te beheersen, werd het daderteam te allen tijde op korte afstand gevolgd door een 'scheidsrechter' die de test kon stilleggen als de situatie te risicovol werd of als de beveiliging intervenieerde. Auditors van de Rekenkamer konden in het observatieteam continu de inbraakpogingen nauwgezet volgen en ontvingen naderhand de ongefilterde rapportage met de resultaten van de test.

Uitkomsten

In totaal zijn er acht testen uitgevoerd bij verschillende locaties, op verschillende tijdstippen en bij verschillende defensieonderdelen. In vier van de acht testen slaagde het daderteam erin de zwaarst beveiligde objecten te bereiken. Daarbij constateerden we dat alle drie soorten beveiligingsniveaus tekortkomingen vertoonden.

De organisatorische beveiligingsmaatregelen gaan ervan uit dat defensiepersoneel zowel de eerste als de laatste beveiligingslinie vormt. De eerste linie omdat beveiliging staat of valt met de alertheid van al het personeel. In de praktijk zagen we die alertheid echter niet. Tot twee keer toe meldde defensiepersoneel niet aan de beveiligingsorganisatie dat ze het daderteam over een hek zagen klimmen. Daarnaast was het defensiepersoneel meermaals behulpzaam bij het lokaliseren van de zwaarst beveiligde objecten door het (undercover) daderteam de weg te wijzen.

Verdere gelegenheid tot het compromitteren van militaire objecten werd geboden doordat personeel niet altijd volgens de regels werkt. Zo waren ruimten met te beveiligen zaken niet goed op slot. De interventieteams van de beveiligingsorganisatie die met honden de laatste beveiligingslinie zijn, reageerden meestal wel op tijd als ze gealarmeerd werden. Echter, omdat zij ook de back-up vormen voor storingen in elektronica of bij tijdelijke huisvesting, is deze organisatie overvraagd en door personeelstekorten onderbezet. Dit maakt dat het defensiepersoneel, ook als

laatste beveiligingslinie, kwetsbaar is.

Bouwkundige staat

De bouwkundige staat van veel defensievastgoed laat te wensen over door slecht inzicht en achterstallig onderhoud, zo constateren we al jaren. Dat geldt ook voor gebouwen waarin beveiligde objecten worden opgeslagen. Defensieonderdelen hebben vaak zelf geen inzicht in deze bouwkundige tekortkomingen. Het herstellen van mankementen aan de gebouwen en de beveiliging daarvan duurt tevens vaak lang. Hierdoor was inbreken bij oude gebouwen in de praktijk mogelijk. Dit gold daarentegen niet voor nieuwbouw. Op een nieuwbouwlocatie slaagde het daderteam er bijvoorbeeld in om ongedetecteerd organisatorische en elektronische beveiligingsmaatregelen te omzeilen, maar was het door bouwkundige maatregelen onmogelijk om in te breken en de militaire objecten daadwerkelijk te bereiken.

Elektronische beveiliging

Voor de elektronische beveiliging maakt Defensie gebruik van 45 verschillende soorten bewakings- en beveiligingssystemen om indringers te detecteren. Veel van deze systemen hebben hun technische levensduur ruimschoots bereikt. Hierdoor zijn ze gevoelig voor storingen en doordat onderdelen schaars worden, duren reparaties lang. Het gevolg is dat ze inboeten aan betrouwbaarheid. Het vervangingsprogramma dat al deze systemen door één nieuw systeem moet vervangen, is echter ernstig vertraagd en in ieder geval niet voor 2025 volledig operationeel.

Zo was het bijvoorbeeld op een zwaarbeveiligd deel mogelijk om via een lang openstaande toegangspoort ongezien mee te liften

Tijdens de test bleek verder dat de huidige elektronische systemen indringers niet altijd signaleerden. Zo was het bijvoorbeeld op een zwaarbeveiligd deel mogelijk om via een lang openstaande toegangspoort ongezien mee te liften. Soms werd detectie genegeerd. Hierdoor was het op diverse defensielocaties mogelijk om de zwaarst beveiligde objecten te beschadigen of te ontvreemden, als het testteam dat had gewild. Alle bevindingen uit de testen hebben we tijdig met het ministerie gedeeld, zodat Defensie passende maatregelen kon nemen. Defensie heeft op ons verzoek ook gecontroleerd of er in de rapportage zaken zijn die de nationale veiligheid schaden, dit was niet het geval.

Op weg naar verbetering

Het grote voordeel van testen in de praktijk is dat je inzicht krijgt in hoe beleid in de werkelijkheid werkt. De kloof tussen een in opzet goede papieren werkelijkheid van beleid en de praktijk wordt zo duidelijk. Door te testen wordt de samenhang tussen verschillende maatregelen ook zichtbaar. Een gebouw kan nog zo goed beveiligd zijn, als er niet veilig gewerkt wordt en ruimten niet worden afgesloten, hebben de bouwkundige investeringen weinig nut. Tegelijkertijd kan de mens wel waakzaam zijn, maar als de elektronische detectie faalt, vaar je toch blind. De waakzaamheid van het defensiepersoneel kun je per slot van rekening alleen in de praktijk vaststellen. Daarom was een van de aanbevelingen van de Algemene Rekenkamer om weer regelmatig in de praktijk te testen of de beveiliging adequaat is. Dat helpt ook om het veiligheidsbewustzijn te verhogen.

Het was goed om te constateren dat nieuwe gebouwen wél bestand zijn tegen inbraakpogingen, dat geeft vertrouwen voor de grote vastgoedoperatie waaraan Defensie net begonnen is. Op basis van je wettelijke taak voor een keer legaal inbreker zijn, is ook gewoon boeiend.

De resultaten van deze audit zijn gepubliceerd en zijn hier te vinden. Dit artikel is geschreven op persoonlijke titel.

Over
Sjoerd Keulen is bijzonder hoogleraar Publieke audit, beleidsevaluatie en verantwoording vanwege de Algemene Rekenkamer, gespecialiseerd in Defensie.

Tom van der Meijden is veiligheidskundige en als auditor van de Algemene Rekenkamer gespecialiseerd in Defensie en Justitie & Veiligheid.

Tags: Veiligheid

Bron url: https://auditmagazine.nl/artikelen/de-auditor-als-inbreker/