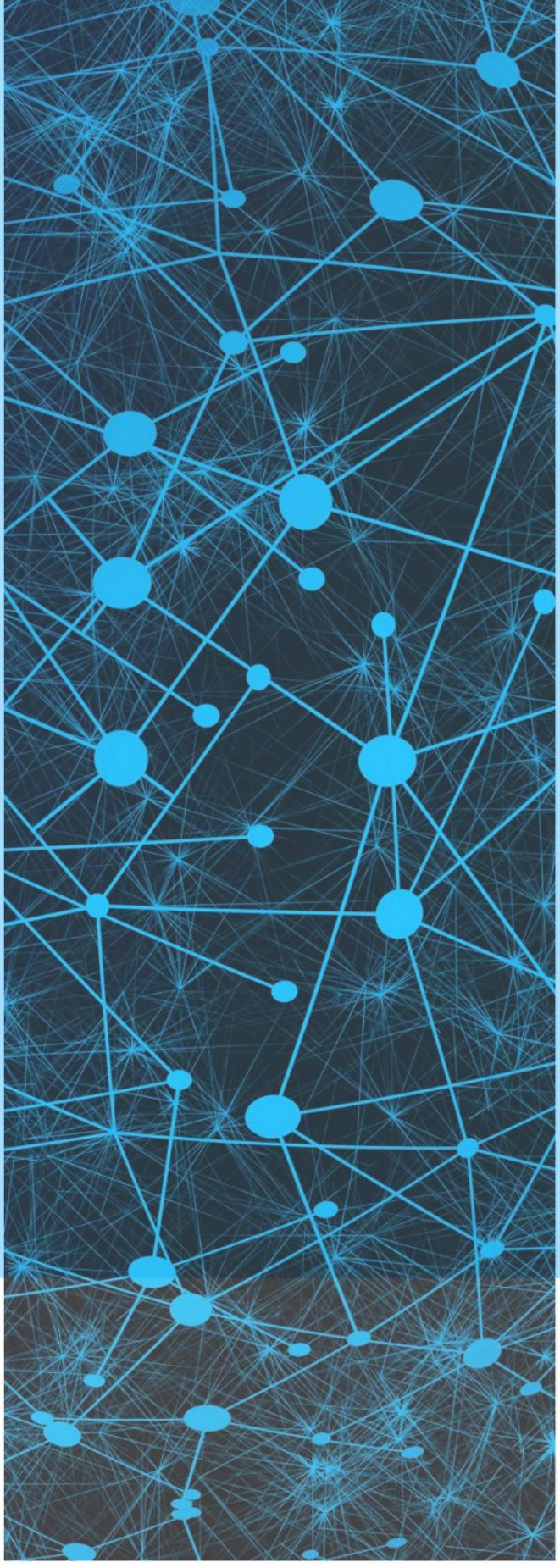
SECURITY MANAGEMENT SYSTEMEN IN NEDERLAND



**Ruben Grijpstra,
Jetske Groot Roessink,
Jos Middelveld,
Niels Rem,
Jesse van Hamburg**

Vereniging Beveiligingsprofessionals Nederland

NDIB
Nationale Denktank Integrale Beveiliging

Voorwoord

Voor u ligt de whitepaper ‘Security Management Systemen in Nederland’. De whitepaper is geschreven in opdracht van de Nationale Denktank Integrale Beveiliging (NDIB) in het kader van het Safety & Security LAB van de opleiding Security Management aan het Saxion te Apeldoorn. Het Safety & Security LAB richt op het analyseren van praktijkgerichte vraagstukken.

Voor het praktijkonderzoek is er een enquête uitgezet onder de leden van de Vereniging Beveiligingsprofessionals Nederland (VBN). Bij deze willen wij hen bedanken voor hun bijdrage. Zonder deze bijdrage hadden wij het rapport niet op deze manier kunnen afronden. Tevens willen wij dhr. Spit en dhr. Hooiveld bedanken voor het uitdagende vraagstuk en de fijne ondersteuning de afgelopen periode.

Wij wensen u informatief leesplezier toe,

Ruben Grijpstra
Jetske Groot Roessink
Jesse van Hamburg
Jos Middelveld
Niels Rem

Apeldoorn, 1 juli 2020

Inleiding

Momenteel heeft de Nationale Denktank Integrale Beveiliging (NDIB) onvoldoende inzicht in de verschillende methodes die security professionals in Nederland gebruiken om tot een Security Management Systeem (SMS) te komen. Naar aanleiding hiervan heeft de NDIB enkele vraagstukken uitgezet die door vijf studenten van het Safety & Security LAB van Hogeschool Saxion in de periode van februari tot en met juni 2020 onder de loep zijn genomen. Het doel hiervan is de kennislacunes in te vullen, om zo professionals meer inzicht te geven in de werking en ervaringen van SMS.

De NDIB is in januari 2012 in het leven geroepen om kennis en informatie over beveiliging en (maatschappelijke) beveiligingsvraagstukken toegankelijk te maken. Hiermee kunnen effectieve en efficiënte publiek-private samenwerkingen en verdere professionalisering van het vakgebied in Nederland worden gestimuleerd. De NDIB werkt aan continue verbetering van geldende wet- en regelgeving, alsmede het verbeteren van de kwaliteit en samenhang van (bestaande) opleidingen in Nederland (devbn, z.d.).

De probleemstelling van het onderzoek luidt als volgt: "*Wat zijn de meest voorkomende Security Management Systemen bij leden van de VBN en op welke wijze, met welke beweegredenen, worden deze door security professionals gehanteerd?"*

Aan de hand van de volgende vijf onderzoeksvragen wordt er antwoord gegeven op de bovenstaande probleemstelling:

- Wat is een Security Management Systeem?
- Welke verschillende soorten Security Management Systemen worden er gebruikt onder de leden van de VBN?
- Hoe worden deze verschillende soorten Security Management Systemen gebruikt onder de leden van de VBN?
- Waarom worden deze Security Management Systemen gebruikt?
- Hoe ervaren leden van de VBN het gebruik van Security Management Systemen?

Om zicht te krijgen op de praktijk is er een enquête uitgezet onder de leden van de VBN. Daarnaast heeft er als toelichting en onderbouwing op de enquête een verdiepend interview plaatsgevonden met een van de respondenten. In deze whitepaper worden de kernpunten en conclusie van het onderzoek beschreven.

Disclaimer: dit onderzoek is opgesteld op basis van de resultaten die zijn voortgekomen uit een enquête die is verspreid onder de leden van de VBN. Helaas hebben wij minder responses ontvangen dan de minimale response rate voor een betrouwbaar onderzoek. De resultaten kunnen daarom niet gegeneraliseerd worden.

Wat is een Security Management Systeem?

Uit ons onderzoek is gebleken dat er geen algemeen geaccepteerde definitie van het begrip Security Management Systeem bestaat. Daarnaast kan er geconcludeerd worden dat er na vergelijking geen eenduidige definitie naar voren komt. Aan de hand van verschillende bronnen is er een algemene, allesomvattende definitie van het begrip SMS ontstaan, welke wordt gehanteerd tijdens het onderzoek. De definitie luidt als volgt:

'Een vastgestelde methode waarmee een organisatie op een gestructureerde wijze het security management proces inricht, uitvoert en onderhoudt om zo tot een adequate beveiliging te komen. Dit Management Systeem is opgesteld met één of meerdere doelen: veiligheid van mensen, Business Continuity, wet- en regelgeving, waarborgen imago, contractuele afspraken met derden, aantoonbaarheid richting toezichthouders, afleggen van verantwoordelijkheid en het beheersen van risico's. Bij dit systeem zijn de volgende stappen onderdeel van het proces en worden getoetst aan de hand van de PDCA-cyclus: het opstellen van een securitybeleid, het maken en onderhouden van risicoanalyses, het opstellen van beveiligingsplannen, het implementeren van maatregelen, het beheren van maatregelen en het evalueren van maatregelen.'

Naast de uitgeschreven definitie is ter ondersteuning een visualisatie ontworpen:

Figuur 1: visualisatie Security Management Systeem

Security management is een doorlopend kwaliteitsproces, waarbij de PDCA-cyclus centraal staat. In de cirkels van de visualisatie zijn de stappen van dit proces puntsgewijs weergegeven. Daarbij komen de verschillende fases van inrichting, uitvoering en onderhoud aan bod. Allereerst stelt een organisatie een securitydoelstellingen op. Op basis van deze doelstellingen wordt het securitybeleid opgesteld.

Vervolgens worden er risicoanalyses uitgevoerd en onderhouden. Aan de hand van de risico's die naar voren komen tijdens de risicoanalyse worden beveiligingsplannen opgesteld (NAVI, 2008). Deze plannen worden ontworpen om de continuïteit van de organisatie te waarborgen tegen (ongewenste) incidenten die door kwaadwillende mensen worden veroorzaakt (Appelman, 2010). Met andere woorden, de risico's worden beheerst. Tot slot wordt het beveiligingsplan geïmplementeerd, beheerd en geëvalueerd. Na de laatste stap begint het proces opnieuw.

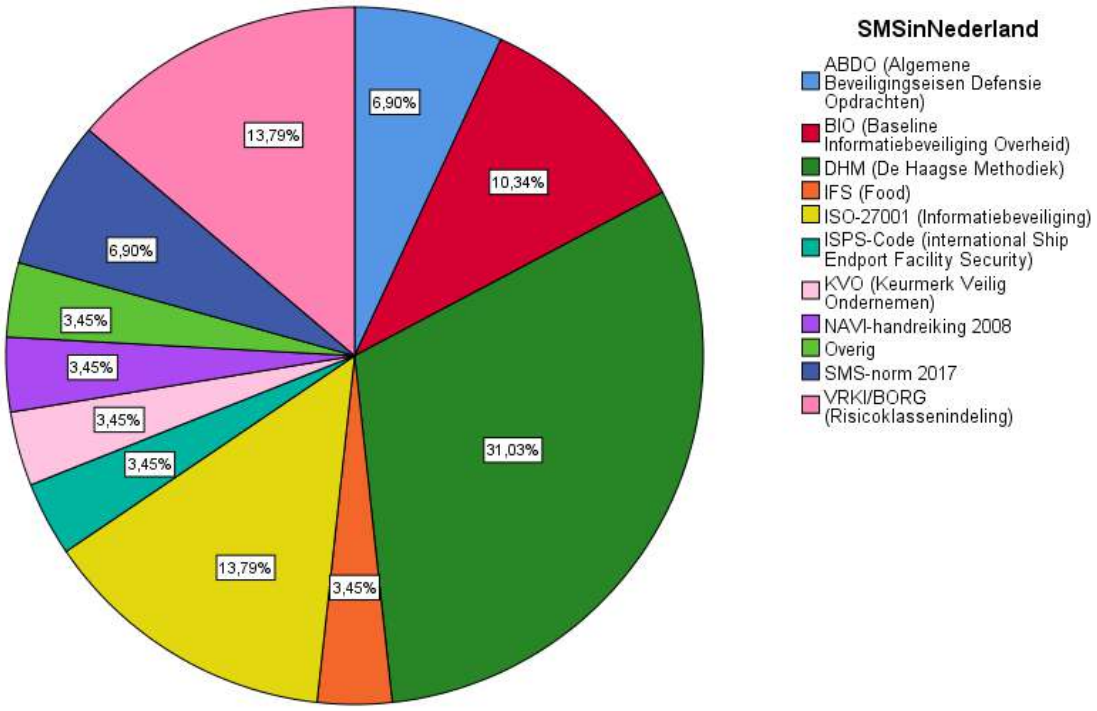
Een Security Management Systeem is opgesteld aan de hand van één of meerdere doelen, voorbeelden hiervan zijn:

- Het waarborgen van de veiligheid van mensen;
- De Business Continuity;
- Verplichte wet- en regelgeving;
- Het waarborgen van het imago van de organisatie;
- Contractuele afspraken met derden;
- Aantoonbaarheid naar toezichthouders;
- Het afleggen van verantwoordelijkheid;
- En het beheersen van risico's.

De definitie en visualisatie zijn tot stand gekomen aan de hand van verschillende bronnen en tekstonderdelen. Het zinsdeel 'Een vastgestelde methode waarmee een organisatie op een gestructureerde wijze het security management proces inricht, uitvoert en onderhoudt' komt voort uit de SMS-norm 2017. Deze zin sluit af met 'om zo tot een adequate beveiliging te komen'. Dit komt voort uit de Algemene Beveiligingseisen voor Defensie Opdrachten 2017 (ABDO). Een management systeem is opgesteld met één of meerdere doelen. De in de definitie genoemde doelen zijn afkomstig uit de ABDO 2017, Authorised Economic Operator 2006 (AEO), Baseline Informatiebeveiliging Overheid 2017 (BIO), BRC Food Safety 2018 en Managementsysteem Integrale Veiligheid 2014 (MIVH). De stappen in het proces worden getoetst aan de hand van de PDCA-cyclus. Dit komt voort uit de BIO 2017, SMS-norm 2017, MIVH 2014 en NAVI-handreiking Risicoanalyse 2008. Tot slot worden de stappen in het proces genoemd, deze zijn afkomstig uit de NAVI-handreiking Risicoanalyse 2008.

Welke verschillende soorten Security Management Systemen worden er gebruikt onder de leden van de VBN?

Er zijn talloze Security Management Systemen op de markt. Soms zijn dit integrale systemen die diverse beveiligingsaspecten behandelen en soms zijn dit systemen die zich enkel op een bepaald onderdeel van beveiliging focussen. Voor een organisatie kan het een lastige afweging zijn of zij een Security Management Systeem willen hanteren en zo ja, welk Security Management Systeem of combinatie van systemen het meest passend zijn.



Figuur 2: Security Management Systemen in Nederland

De resultaten die zijn voortgekomen uit het onderzoek zijn als volgt (zie figuur 2):

- 31,03% van de respondenten maakt gebruik van 'De Haagse Methodiek (DHM)';
- 13,79% van de respondenten maakt gebruik van de 'ISO-27001' ten behoeve van informatiebeveiliging;
- 13,79% van de respondenten maakt gebruik van de 'VRKI/BORG Risicoklasse-indeling';
- 10,34% van de respondenten maakt gebruik van de 'Baseline Informatiebeveiliging Overheid';
- 6,90% van de respondenten maakt gebruik van de 'Algemene Beveiligingseisen Defensie Opdrachten (ABDO)';
- 6,90% van de respondenten maakt gebruik van de 'SMS-Norm 2017';
- 3,45% van de respondenten maakt gebruik van het 'Keurmerk Veilig Ondernemen (KVO)';
- 3,45% van de respondenten maakt gebruik van de 'International Ship and Port facility Security Code (ISPS)';
- 3,45% van de respondenten maakt gebruik van de 'NAVI Handreiking 2008';
- 3,45% van de respondenten maakt gebruik van de 'IFS Food';
- 3,45% van de respondenten maakt gebruik van 'overige' Security Management Systemen.

Opvallend aan de resultaten is het brede gebruik van 'De Haagse Methodiek' in vergelijking met andere Security Management Systemen. Grofweg een derde van alle respondenten gebruikt De Haagse Methodiek binnen de organisatie. Dit komt overeen met de data uit het verdiepende interview dat is gehouden met een lid van de VBN. De geïnterviewde respondent deed de uitspraak 'De Haagse Methodiek wordt erg breed gedragen en gebruikt door beveiligend Nederland' (persoonlijke communicatie, 2020). Deze uitspraak wordt ondersteund door de resultaten uit de enquête.

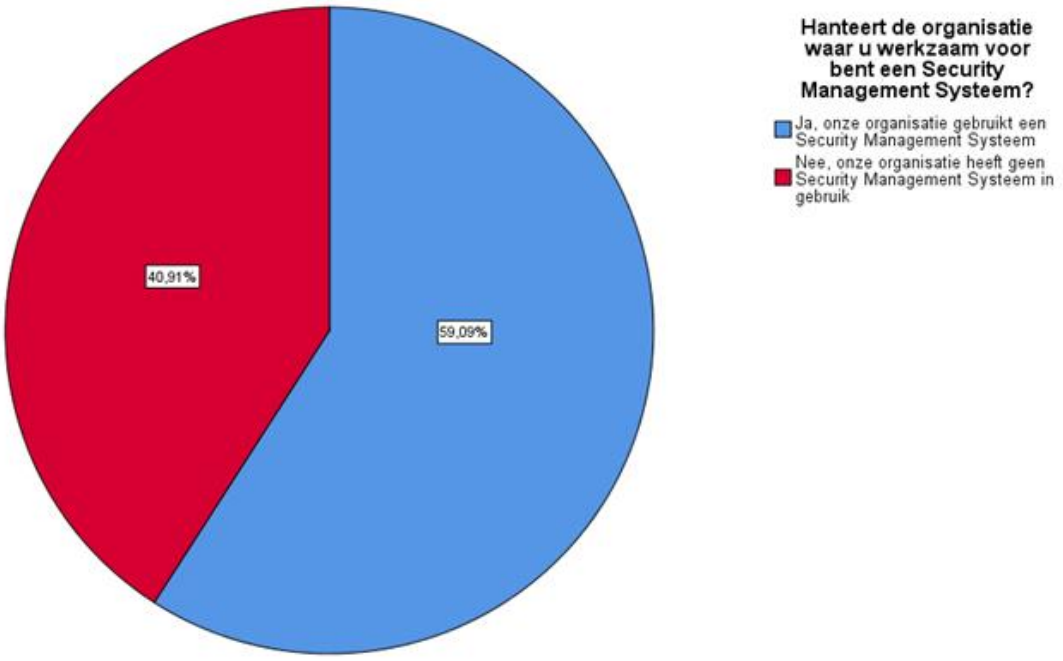
Naast de inventarisatie van welke Security Management Systemen er gehanteerd worden onder leden van de VBN, is er ook onderzoek gedaan naar welke Security Management Systemen gebruikt worden in welke sectoren (zie figuur 3). Dit geeft inzicht in hoe breed een Security Management Systeem gebruikt wordt in Nederland. Zo is te zien dat sommige systemen enkel in één specifieke sector worden gehanteerd, terwijl andere systemen binnen veel verschillende sectoren worden gebruikt. Een voordeel van een systeem dat voornamelijk gebruikt wordt binnen één sector, is dat het systeem erg toepasbaar is op deze specifieke sector. Een nadeel hiervan is dat het systeem lastiger te vergelijken of te integreren is met systemen die veel worden toegepast in andere sectoren. Systemen die binnen veel sectoren toegepast worden geven over het algemeen minder concrete maatregelen voor organisaties. Dit kan worden gezien als een voordeel, er is namelijk meer ruimte om zelf invulling te geven aan maatregelen. Echter kan dit ook gezien worden als een nadeel, er moet namelijk beter nagedacht worden welke maatregelen passend zijn voor de eigen organisatie.

Kruistabel gebruik SMS per sector

		Sector							Totaal
		Anders	Consultancy	Handel en dienstverlening	ICT	Justitie, veiligheid en openbaar bestuur	Onderwijs, cultuur en wetenschap	Techniek, productie en bouw	
SMS	ABDO (Algemene Beveiligingseisen Defensie Opdrachten)			50,0%		50,0%			100,0%
	BIO (Baseline Informatiebeveiliging Overheid)		33,3%			66,7%			100,0%
	DHM (De Haagse Methodiek)	11,1%	22,2%	11,1%	11,1%	33,3%		11,1%	100,0%
	IFS (Food)			100,0%					100,0%
	ISO-27001 (Informatiebeveiliging)		75,0%	25,0%					100,0%
	ISPS-Code (international Ship Endport Facility Security)		100,0%						100,0%
	KVO (Keurmerk Veilig Ondernemen)			100,0%					100,0%
	NAVI-handreiking 2008		100,0%						100,0%
	Overig						100,0%		100,0%
	SMS-norm 2017		50,0%			50,0%			100,0%
	VRKI/BORG Risicoklassenindeling		25,0%	75,0%					100,0%
Totaal		3,4%	34,5%	27,6%	3,4%	24,1%	3,4%	3,4%	100,0%

Figuur 3: Kruistabel gebruik Security Management Systeem per sector

Organisaties kiezen er dus regelmatig voor om een Security Management Systeem te gebruiken voor de inrichting van de beveiliging. Echter is er ook een gedeelte dat ervoor kiest om geen Security Management Systeem te hanteren. Ruim 40 procent van de respondenten die de enquête heeft ingevuld gaf aan geen Security Management Systeem te hanteren binnen de organisatie. De meerderheid, 59,09% van de respondenten, heeft aangegeven wel gebruik te maken van een Security Management Systeem.



Figuur 4: Hanteren Security Management Systeem

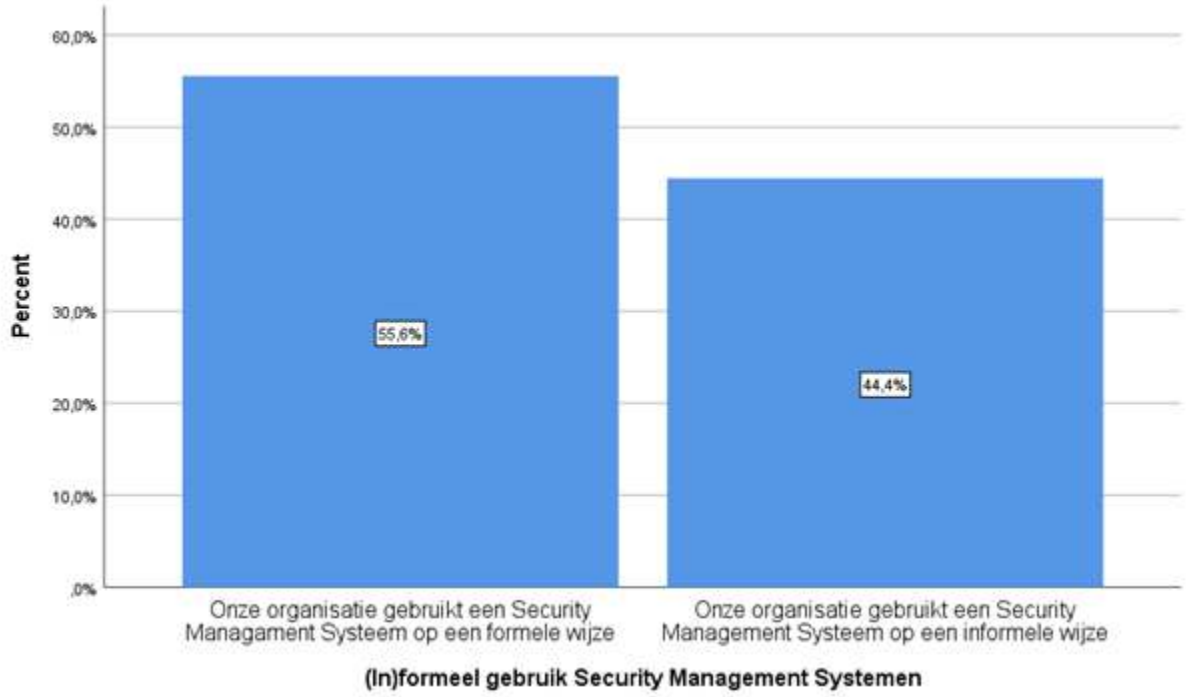
Geconcludeerd kan worden dat het aantal respondenten dat gebruik maakt van een Security Management Systeem geen ruime meerderheid vormt. Dit betekent dat Security Management Systemen nog niet door heel beveiligend Nederland gedragen worden als middel om de beveiliging binnen de organisatie in te richten.

Hoe worden deze verschillende soorten Security Management Systemen gebruikt onder de leden van de VBN?

Security Management Systemen zijn op meerdere manieren te gebruiken. Een professional kan ervoor kiezen om een Security Management Systeem precies volgens het boekje te volgen, maar ook bepaalde modellen uitkiezen uit een Security Management Systeem behoort tot de mogelijkheden. Verder kan ervoor gekozen worden om een Security Management Systeem formeel te gebruiken binnen de organisatie of juist het tegenovergestelde: informeel. In de context van dit onderzoek kunnen deze twee termen als volgt worden beschreven:

- **Formeel:** Het Security Management Systeem is vastgelegd in beleidsstukken.
- **Informeel:** Het Security Management Systeem is niet vastgelegd in beleidsstukken, er wordt wel een vrije vorm van security management gehanteerd.

Uit de resultaten van de enquête blijkt dat 55,6% van de Security Management Systemen formeel wordt gebruikt. Daar staat tegenover dat 44,4% van de Security Management Systemen informeel wordt gebruikt.



Figuur 5: (In)formeel gebruik Security Management Systemen

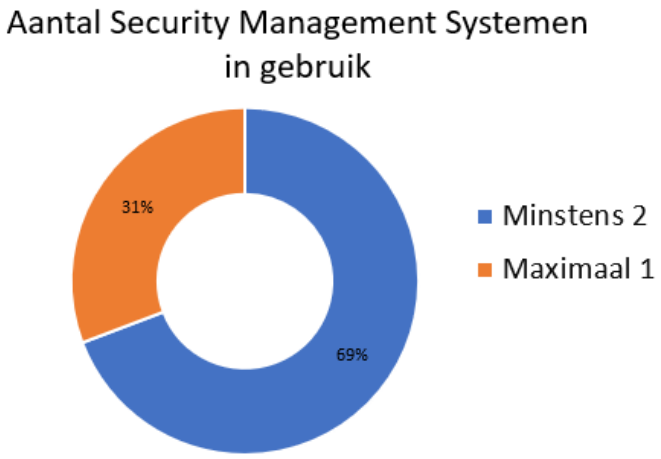
Verder blijkt uit de resultaten van de enquête dat de mate van het (in)formele gebruik verschilt per Security Managent Systeem. In de onderstaande tabel is te zien hoe de specifieke Security Management Systemen gebruikt worden door de respondenten:

Formeel/informeel

		Geïmplementeerde wijze		
		Onze organisatie gebruikt een Security Management Systeem op een formele wijze	Onze organisatie gebruikt een Security Management Systeem op een informele wijze	Total
SMS	ABDO (Algemene Beveiligingseisen Defensie Opdrachten)	100,0%		100,0%
	BIO (Baseline Informatiebeveiliging Overheid)	66,7%	33,3%	100,0%
	DHM (De Haagse Methodiek)	87,5%	12,5%	100,0%
	IFS (Food)		100,0%	100,0%
	ISO-27001 (Informatiebeveiliging)	25,0%	75,0%	100,0%
	ISPS-Code (international Ship Endport Facility Security)		100,0%	100,0%
	KVO (Keurmerk Veilig Ondernemen)		100,0%	100,0%
	NAVI-handreiking 2008		100,0%	100,0%
	SMS-norm 2017	50,0%	50,0%	100,0%
	VRKI/BORG (Risicoklassenindeling)	50,0%	50,0%	100,0%
Totaal		55,6%	44,4%	100,0%

Figuur 6: Formeel/Informeel gebruik

Wat opvalt uit figuur 6 is dat de ISPS-code, het KVO, de IFS en de NAVI-handreiking door de respondenten slechts informeel worden gebruikt. De ABDO daarentegen wordt slechts formeel gebruikt. Bij sommige systemen is het om het even, bij andere systemen is er een groot verschil aanwezig tussen het formele en informele gebruik, terwijl deze systemen zowel formeel als informeel gebruikt worden.



Figuur 7: Aantal Security Management Systemen in Gebruik

Tot slot blijkt dat Security Management Systemen als aanvulling op elkaar worden gebruikt. Veel systemen zijn op bepaalde vlakken niet uitgebreid genoeg. De combinatie van twee of meer systemen kan dan helpen. Cijfers uit de enquête tonen aan dat ongeveer zeven op de tien respondenten gebruik maakt van minstens twee Security Management Systemen, zie hiervoor figuur 7. Het aantal systemen dat de respondenten in gebruik hebben varieert van één tot vijf, waarbij de meeste respondenten twee systemen in gebruik hebben.

Waarom worden deze Security Management Systemen gebruikt?

Er kunnen verschillende redenen ten grondslag liggen aan de keuze voor een bepaald Security Management Systeem. Bij het invullen van de enquête kregen de respondenten vijf keuzes als motivatie voor het hanteren van een bepaald systeem, namelijk;

1. De sector hanteert de norm;
2. Waarborgen van het imago;
3. Contractuele verplichtingen;
4. Verplichte wet- en regelgeving;
5. Overig.

Indien de motivatie van de respondent onder geen van de gegeven opties viel, kreeg hij of zij de mogelijkheid om deze in te vullen bij overig. In figuur 8 is een kruistabel weergegeven die het verband weergeeft tussen de verschillende Security Management Systemen en de motivatie voor de keuze van het betreffende SMS. Op de verticale as zijn de Security Management Systemen weergegeven die worden gehanteerd door de respondenten. Op de horizontale as zijn de bijbehorende motivaties weergegeven.

Motivatie gebruik Security Management Systemen

		Motivatie					
		De sector hanteert deze norm	Dit doen wij om ons imago te waarborgen	Overig	Wij zijn dit als organisatie contractueel verplicht	Wij zijn dit als organisatie verplicht vanuit de wetgeving	Totaal
SMS	ABDO				100,0%		100,0%
	BIO		33,3%			66,7%	100,0%
	DHM	50,0%	16,7%	33,3%			100,0%
	IFS	100,0%					100,0%
	ISO-27001		50,0%			50,0%	100,0%
	ISPS-Code	100,0%					100,0%
	KVO		100,0%				100,0%
	NAVI Handreiking 2008		100,0%				100,0%
	Overig	100,0%					100,0%
	SMS-norm 2017		50,0%	50,0%			100,0%
	VRKI/BORG	50,0%				50,0%	100,0%
Totaal		30,8%	30,8%	11,5%	3,8%	23,1%	100,0%

Figuur 8: motivatie gebruik Security Management Systemen

In zijn algemeenheid kan worden geconcludeerd dat 30,8% van de respondenten die gebruik maakt van een Security Management Systeem als reden opgeeft dat zij een SMS hanteren in verband met de door de sector gehanteerde norm. Het aantal respondenten dat dit doet vanuit het oogpunt om hiermee het imago van de organisatie te waarborgen ligt ook op 30,8%. Een relatief klein aantal van de respondenten (3,8%) hanteert een Security Management Systeem omdat zij dit contractueel verplicht zijn. Uit figuur 8 is af te leiden dat hier onder de respondenten alleen sprake van is bij de ABDO. Ook verplichtingen vanuit de wet- en regelgeving is bij 23,1% van de respondenten die gebruik maakt van een Security Management Systeem een motivatie om een bepaalde norm te hanteren.

11,5% van de respondenten die een Security Management Systeem in gebruik heeft doet dit met overige redenen. De overige reden bij De Haagse Methodiek is dat dit een bewezen systeem is. Een andere overige reden is dat een systeem wordt gebruikt als aanvulling op een ander systeem. Dit is van toepassing bij de SMS-norm 2017.

De twee voornaamste redenen dat respondenten kiezen voor een Security Management Systeem is dus omdat de sector de norm hanteert of omdat zij hiermee het imago van de organisatie waarborgen. Interessant is dat hieruit blijkt dat er een evenredig verhouding is tussen verplichtingen die organisaties opgelegd krijgen en de verantwoordelijkheid die organisaties zelf nemen ten aanzien van security management.

Hoe ervaren leden van de VBN het gebruik van Security Management Systemen?

Uit het onderzoek is gebleken dat de gebruikte Security Management Systemen scoren tussen een 5 en een 8,5. De score is bepaald aan de hand van de enquête die is verspreid onder de leden van de VBN. Van de gegeven scores is het gemiddelde berekend. Een aantal Security Management Systemen zijn bij de beoordeling buiten beschouwing gelaten (ISPS-Code & NAVI-handreiking). De reden hiervoor is dat deze Security Management Systemen door de respondenten in een kleiner aantal zijn beoordeeld op de doeltreffendheid en gebruiksvriendelijkheid.

	Gemiddeld cijfer doeltreffendheid	Gemiddeld cijfer gebruiksvriendelijkheid
ABDO	7,5	6
BIO	6,7	6,4
DHM	8	7,7
IFS	6	5
ISO 27001	7,6	6,5
KVO	7	7
SMS-norm 2017	8,5	8,5
VRKI/BORG	7,5	7,5

Figuur 9: Cijfers Security Management Systemen

Zowel op doeltreffendheid als gebruiksvriendelijkheid (8.5 & 8.5) is de SMS-norm 2017 als hoogst beoordeeld. Dit komt voornamelijk door het feit dat dit systeem gebruikt kan worden om een integraal security beleidsplan op te stellen. Het is erg duidelijk omschreven, waardoor men geen vertaalslag hoeft te maken naar andere afdelingen binnen de organisatie. Doordat het gebruikt kan worden om een integraal security beleidsplan op te stellen, is het een heel breed opgesteld document. Dit is zowel een voordeel als een nadeel. Integrale security beleidsplannen bevatten namelijk alle onderdelen van een organisatie met betrekking tot de bedrijfsprocessen en assets.

DHM (De Haagse Methodiek) is na de SMS-norm 2017 als hoogste uit het onderzoek gekomen op het gebied van zowel doeltreffendheid als gebruiksvriendelijkheid (8 & 7.7). Dit komt voornamelijk door de alomvattende aanpak van DHM. Daarnaast resulteert DHM in eenzelfde taal die wordt gesproken omtrent security binnen en tussen organisaties. Daarnaast innoveert DHM mee met de tijd, het leerprogramma wordt vaak geüpdatet. Gebleken is dat men aan de hand van de PDCA-cyclus security doelen kan behalen, het biedt een basisstructuur. Zonder een norm en structuur wordt de security scope snel te breed en/of te diep.

De IFS (Food) komt als laagst beoordeelde systeem uit het onderzoek op het gebied van doeltreffendheid en gebruiksvriendelijkheid (6 & 5). Dit is een Security Management Systeem dat een norm weergeeft voedselveiligheid. De score is relatief laag, omdat de IFS niet specificeert hoe processen binnen de productieketen vormgegeven dienen te worden. Dit houdt in dat er een hoge mate van flexibiliteit is binnen de standaard. Hierdoor kunnen er grote verschillen optreden in de mate van beveiliging tussen de verschillende gecertificeerde organisaties.

Conclusie

In de inleiding van de whitepaper werd de volgende probleemstelling geïntroduceerd: "*Wat zijn de meest voorkomende Security Management Systemen bij leden van de VBN en op welke wijze, met welke beweegredenen, worden deze door security professionals gehanteerd?"* Om antwoord te geven op deze vraag is zowel kwalitatief- als kwantitatief onderzoek uitgevoerd.

Uit de resultaten van de literatuurstudie is gebleken dat er geen algemeen geaccepteerde definitie van het begrip Security Management Systeem bestaat. Daarnaast kan er geconcludeerd worden dat er na vergelijking geen eenduidige definitie naar voren komt. Aan de hand van verschillende bronnen is de volgende algemene, allesomvattende definitie ontstaan:

'Een vastgestelde methode waarmee een organisatie op een gestructureerde wijze het security management proces inricht, uitvoert en onderhoudt om zo tot een adequate beveiliging te komen. Dit Management Systeem is opgesteld met één of meerdere doelen: veiligheid van mensen, Business Continuïty, wet- en regelgeving, waarborgen imago, contractuele afspraken met derden, aantoonbaarheid richting toezichthouders, afleggen van verantwoordelijkheid en het beheersen van risico's. Bij dit systeem zijn de volgende stappen onderdeel van het proces en worden getoetst aan de hand van de PDCA-cyclus: Het opstellen van een securitybeleid, het maken en onderhouden van risicoanalyses, het opstellen van beveiligingsplannen, het implementeren van maatregelen, het beheren van maatregelen en het evalueren van maatregelen.'

Aan de hand van de bovenstaande definitie is een enquête verspreid onder de leden van de VBN over het gebruik van Security Management Systemen. Uit de resultaten van de enquête kan worden geconcludeerd dat de meerderheid van de respondenten een SMS gebruikt. Opvallend hierbij is het brede gebruik van 'De Haagse Methodiek'. Grofweg een derde van alle respondenten gebruikt De Haagse Methodiek binnen de organisatie. Dit komt overeen met de data uit het verdiepende interview dat is gehouden met een van de leden van de VBN. De geïnterviewde respondent deed de uitspraak: 'De Haagse Methodiek wordt erg breed gedragen en gebruikt door beveiligend Nederland' (persoonlijke communicatie, 2020). Ondanks dat de meerderheid van de respondenten wel een SMS gebruikt, is er nog steeds een grote groep die hier geen gebruik van maakt. Security Management Systemen worden dus niet gedragen door heel beveiligend Nederland als middel om beveiliging in te richten.

Uit de enquête blijkt dat de meeste respondenten twee of meer systemen gebruiken. Op basis hiervan kan worden geconcludeerd dat één Security Management Systeem in de meeste gevallen niet toereikend genoeg is. Een kleine meerderheid van de respondenten gebruikt de systemen op een formele wijze. Daarnaast worden een aantal Security Management Systemen uitsluitend op een informele of formele wijze gebruikt. De twee voornaamste redenen dat respondenten kiezen voor een dergelijk systeem is omdat de sector de norm hanteert of omdat zij hiermee het imago van de organisatie waarborgen. Geconcludeerd kan worden dat er dus een evenredige verhouding is tussen verplichtingen die organisaties opgelegd krijgen en de verantwoordelijkheid die organisaties zelf nemen ten aanzien van security management. Daarnaast zijn er door de respondenten twee overige redenen opgegeven als motivatie voor het gebruik van DHM en de SMS-norm 2017, namelijk: DHM is een bewezen systeem en de SMS-norm 2017 wordt gebruikt als aanvulling op DHM.

Zowel op doeltreffendheid als op gebruiksvriendelijkheid scoort de SMS-norm 2017 het hoogst. Dit komt voornamelijk door het feit dat het gebruikt kan worden om een integraal security beleidsplan op te stellen. De omschrijving zorgt ervoor dat men geen vertaalslag hoeft te maken naar andere afdelingen binnen de organisatie. Na de SMS-norm 2017 komt DHM (De Haagse Methodiek) het beste uit het onderzoek. Dit komt voornamelijk door de alomvattende aanpak van DHM.

Literatuurlijst

ABDO. (2017, 13 juni). ABDO 2017. Geraadpleegd op 6 mei 2020, van https://www.defensie.nl/downloads/beleidsnota-s/2017/06/13/abdo-2017

AEO. (2006, 13 juni). The AEO Compact Model. Geraadpleegd op 6 mei 2020, van https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/policy_issues/customs_security/aeo_compact_model_en.pdf

BIO 1.04. (2020, 6 januari). Baseline Informatiebeveiliging Overheid. Geraadpleegd op 6 mei 2020, van https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

BRC Food Safety. (2018, augustus). Global Standard Food Safety. Geraadpleegd op 6 mei 2020, van https://www.scsglobalservices.com/files/program_documents/brc_food_standard_8.pdf

Devbn. (z.d.). Nationale Denktank Integrale Beveiliging. Geraadpleegd op 10 juni 2020, van https://devbn.nl/nl/activiteiten/nationale-denktank-integrale-beveiliging

MIVH. (2019, 26 juni). Managementsysteem Integrale Veiligheid (MIVH). Geraadpleegd op 15 juni 2020, van https://www.integraalveilig-ho.nl/instrument/managementsysteem-integrale-veiligheid-mivh/

NAVI. (2008). Handreiking Risicoanalyse: 10 praktische modellen voor de risicoanalist. Geraadpleegd op 6 mei 2020, van https://cyberwar.nl/d/2008_NAVI-Handreiking-Risicoanalyse_10-praktische-modellen-voor-de-risicoanalist.pdf

Spit, M. (2017). Security Management Systeem Norm 2017 [PDF] (Vol. 2017). Geraadpleegd van https://play.google.com/books/reader?id=6-pGDwAAQBAJ&pg=GBS.PA1